# RFID – Säkerhet och integritet

E M M A  A N G E R M U N D
o c h  E M M A  L I N D Q V I S T


KTH Datavetenskap
och kommunikation

Examensarbete
Stockholm, Sverige 2011

# RFID – Säkerhet och integritet

E M M A  A N G E R M U N D
o c h  E M M A  L I N D Q V I S T

Examensarbete i datalogi om 15 högskolepoäng
vid Programmet för datateknik
Kungliga Tekniska Högskolan år 2011
Handledare på CSC var Mads Dam
Examinator var Mads Dam

URL: www.csc.kth.se/utbildning/kandidatexjobb/datateknik/2011/angermund_emma_OCH_lindqvist_emma_K11039.pdf

Kungliga tekniska högskolan
*Skolan för datavetenskap och kommunikation*

**KTH** CSC
100 44 Stockholm

URL: www.kth.se/csc

## Abstract

RFID is a technology for identification of a variety of things ranging from pets, containers and passports to keys. The fast development and implementation has resulted in problems concerning security and integrity. These problems have been debated and then set aside due to the increased cost the improved level of security and safety with more advanced technology would mean.

This report will discuss the problems with RFID technology based on a simple experiment of copying RFID tags that are used as apartment keys in a large student complex in Stockholm, Sweden. The simplicity of copying the tags arose multiple questions concerning the use and the small amount of knowledge the users have about the tags weaknesses and the way they function. The study focus on integrity and security questions and discuss the advantages and disadvantages of using RFID technology. Also possible solutions to the problems with RFID will be suggested.

## Sammanfattning

RFID är en teknik som används för identifiering inom en mängd olika områden, till exempel husdjur, containrar, pass och nycklar. Den snabba utvecklingen och det utbredda användandet har resulterat i säkerhets- och integritetsproblem. Dessa problem har diskuterats, men sedan åsidosatts på grund av de ökade kostnader som uppstår i samband med den mer avancerade teknik som krävs för den förbättrade säkerheten.

Rapporten berör RFID-teknologins problem utifrån ett enkelt experiment där lägenhetsnycklar till ett stort studentkomplex i Stockholm kopierades. Att det var så enkelt att kopiera nycklarna väckte flera frågor angående användarnas bristande kunskap och nycklarnas svagheter. Studien fokuserar på RFID-teknikens integritets- och säkerhetsfrågor samt diskuterar dess för- och nackdelar. Även möjliga lösningar på problemen föreslås.

# Innehåll

# 1 Inledning

Denna rapport ger en beskrivning av RFID-tekniken och dess användningsområden. Fokus ligger på att diskutera de säkerhets- och integritetsproblem som finns. Kring säkerhetsproblematiken genomförs även ett praktiskt experiment för att belysa dessa problem ytterligare. Inledningsvis beskrivs rapportens syfte, en problemformulering samt en dokumentöversikt.

Rapporten har skrivits som ett kandidatexamensarbete vid CSC-skolan på Kungliga Tekniska Högskolan i Stockholm av Emma Angermund och Emma Lindqvist. Inledningsvis delades de olika huvudrubrikerna upp mellan de båda författarna, men eftersom utkasten till de olika delarna har bearbetats så många gånger av båda två, kan all text i rapporten ses som gemensam. Även experimenten genomfördes tillsammans.

## 1.1 Syfte

RFID är en kommunikationsteknik som med hjälp av radiovågor skickar information mellan en läsare och en sändare. Teknologin är idag vitt spridd och används för identifikation av människor, djur och saker. Utvecklingen av RFID har gått fort, och som med mycket annan ny teknik har säkerhets- och integritetsfrågorna kommit i skymundan. Syftet med den här rapporten är att utreda eventuella säkerhetsbrister med RFID och undersöka om det är relevant med en förnyad integritetsdebatt.

## 1.2 Problemformulering

I rapporten belyses RFID-tekniken ur ett säkerhets- och integritetsperspektiv. Problem med tekniken och eventuella lösningar på dessa presenteras.

Genom praktiska försök kartläggs RFID-användningen i form av nyckelbrickor hos personer bosatta i Stockholmsområdet. Utifrån en säkerhetsaspekt undersöktes hur lätt det är att kopiera dessa nycklar, samt hur förutsägbart nycklarnas innehåll är. Med integritetsaspekten som utgångspunkt ställdes frågan till fastighetsförvaltare hur användandet av nyckelbrickorna loggas.

Det problematiseras kort kring huruvida en fientlig person eller organisation skulle kunna spåra individer i olika situationer, till exempel genom att plantera ut RFID-läsare på rätt ställen, använda sig av bärbara RFID-läsare eller använda redan befintlig utrustning för att lyssna av och/eller logga användare.

De konkreta frågor som är besvarade är listade nedan.

- Hur fungerar RFID-teknologin?
- Hur utbrett är användningsområdet för RFID-teknologin?
- Hur anonymt är RFID-teknologin i dagsläget?
- Vilka säkerhetsproblem har dykt upp under tiden de funnits?
- Hur mycket säkerhetstänkande har fastighetsförvaltare som använder RFID-teknologin till nycklar i sina fastigheter?
- Hur kan säkerheten utvecklas och förstärkas?

Under arbetets gång har nya frågeställningar ständigt dykt upp som vi funnit relevanta att utforska vidare, men utgångspunkten var de frågor som listats ovan.

### 1.3 Dokumentöversikt

Efter inledningen presenterar rapporten under de två första avsnitten RFID-teknikens bakgrund och grundläggande begrepp under. Där kommer även olika typer av taggar att beskrivas. Avsnitt tre och fyra berör säkerhetsproblem respektive integritetsproblem, för att ge struktur och tydlighet i dessa problem separeras olika typer av problem i olika underrubriker. Avsnitt fem behandlar förslag till lösningar på de problem som beskrivits i del tre och fyra. Även här förklaras olika lösningar i olika delar.

Avsnitt sex presenterar de metoder som använts under studien och hur utförandet gått till. Avsnitt sju beskriver de resultat som studien har resulterat i, och i avsnitt åtta förs en diskussion kring studiens resultat. Diskussionen betonar de säkerhets- och integritetsproblem som rapporten tagit upp samt ger förslag på förbättringar inom dessa områden. Rapporten avslutas med en referens- och figurförteckning.

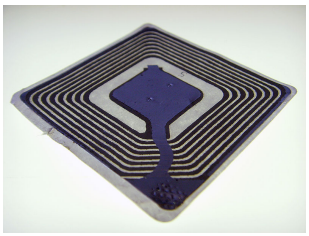
# 2 Bakgrund

För att få en djupare förståelse för hur RFID-tekniken fungerar följer här först en kort introduktion till tekniken och därefter en mer grundlig beskrivning inriktad på olika radiofrekvenser, minnestyper samt typer av taggar. Slutligen presenteras några olika användningsområden.

## 2.1 Introduktion till RFID-teknologin

RFID, Radio Frequency Identification, är en kommunikationsteknik där ingen fysisk eller synlig kontakt behövs. En läsare och en elektronisk sändare, som kallas för tagg, kommunicerar med hjälp av radiovågor. Läsaren skickar i sin tur vidare informationen till en värddator som tolkar den. RFID-tekniken liknar på många sätt tekniken som används av streckkoder. En viktig skillnad i praktiken är att taggarna oftast identifierar en unik produkt, medan streckkoderna identifierar en grupp av varor. Tekniken sägs ha sina rötter i radarrelaterad forskning som skedde under andra världskriget [28], men det var först 1973 som de första RFID-patenten togs i USA [1] [2].

I de enklaste fallen skickar RFID-läsaren ut en radiosignal, som aktiverar taggen, varpå taggen svarar genom att skicka tillbaka information till läsaren. Informationen behandlas därefter av en dator. Ett RFID-system består alltså av tre huvudkomponenter: läsaren, taggen och värddatorn. Taggen består av en antenn som tar upp radiosignalen samt ett mikrochip där data lagras [3], se figur 1. Mikrochipets minnescell kan vara av typ a, som innebär att det bara kan läsas, eller av typ b, som också är skrivbar [4].



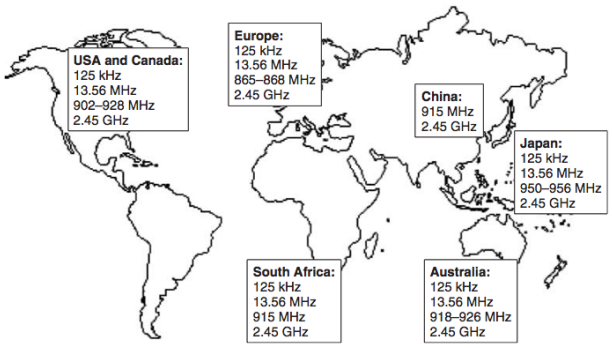
Figur 1: En tagg med antenn och mikrochip. Källa: [26]

## 2.2 Olika radiofrekvenser

RFID använder ett brett spektrum av radiofrekvenser, från 125kHz upp till 5.8GHz[1]. Olika världsdelar tillåter olika frekvenser för RFID-kommunikation, se figur 2. I *RFID for the Optimization of Business Processes* listar Wolf-Ruediger Hansen och Frank Gillert fyra prestandaparametrar som varierar beroende på val av frekvens [22]:

- kommunikationsavstånd
- dataöverföringshastighet
- lämplighet för avläsning av flera taggar samtidigt
- känslighet för påverkan från omgivande föremål

De högre frekvenserna klarar av en snabbare dataöverföring och ofta längre kommunikationsavstånd, men är å andra sidan inte lika tåliga för yttre påverkan från exempelvis metall och vatten som kan störa radiovågorna. De olika frekvensområdena[2] har därmed både sina för- och nackdelar och används för olika ändamål [19] [20]. Taggar som har en egen strömförsörjning kan kommunicera över betydligt längre avstånd än de som får sin strömförsörjning tillgodosedd genom att omvandla läsarens utsända radiosignal till elektricitet [4].




Figur 2: Tillåtna frekvensomfång i olika världsdelar. Källa: [22]

[1] Vissa frekvensområden har protokoll och teknik definierade i ISO/IEC 18000 Part 1-7 [5].

[2] Det finns ett antal telekommunikationsfrekvensområden som har namngetts av ITU, FN-organet för information- och kommunikationsteknologi, som även RFID kan kategoriseras utifrån [21].

### Lågfrekvens

Dessa taggar kommunicerar över frekvensområdet under 135kHz. De har ett kommunikationsavstånd på ett par centimeter, vilket inte är särskilt långt, men påverkas minst av yttre omständigheter såsom inverkan från vatten och metall. Vanliga användningsområden är passerkort, märkning av djur och produktautentisering.

### Högfrekvens

Dessa taggar kommunicerar över 13,56MHz. De kan klara av både längre kommunikationsavstånd och högre överföringshastighet än lågfrekvenstaggarna. Läsavståndet för dessa taggar kan vara upp till en meter. Antennen behöver inte heller vara lika stor som för de med lägre frekvens, varför taggarna kan vara mindre. Högfrekvenstaggarna är därför billiga att tillverka. Däremot är de mer känsliga för påverkan av yttre omständigheter. De används bland annat i biblioteksböcker och i resebevis.

### Ultrahögfrekvens

Dessa taggar kommunicerar över frekvensområdet 860MHz-960MHz. De har ett kommunikationsavstånd till uppemot tre meter och dataöverföringshastigheten är snabbare än för högfrekvenstaggarna, däremot påverkas de mer av omgivande vatten eller metall. Många gånger skiljer sig dock läsarens och taggens kommunikationsavstånd åt. I vissa fall kan läsaren skicka signaler till en tagg på upp till 100 meters avstånd, medan informationen som kommer tillbaka från taggen bara kan färdas ett par meter [13]. Vanliga användningsområden är pall- och kartongspårning, tillgång till parkering och vägtullsinsamling.

### Mikrovågor

Dessa taggar kommunicerar över frekvensområdet 2.45GHz-5.8GHz, även kallat superhög frekvens. Mikrovågstaggarna har den högsta överföringshastigheten, och har ett kommunikationsavstånd på upp till en meter. Sändningen blockeras däremot lätt av omgivande metallföremål och vatten. De är också väldigt dyra, varför användningen än så länge mest är koncentrerad till märkning av flygplansbagage och elektronisk tullinsamling.

## 2.3 Olika minnestyper

Hur stor minneskapacitet en tagg har varierar beroende på pris och tänkt användningsområde, och det finns både taggar som endast är läsbara och de som är läs- och skrivbara. Förutom de taggar som har olika typer av minne som går att läsa och ibland skriva, finns det även taggar som har mer ”aktiv elektronik”, en egen liten processor, som kan utföra olika små funktioner.

Taggar med litet lagringsutrymme som bara kan läsas är billigast att tillverka, och därmed även vanligast förekommande [23]. Storleken på minnet varierar, men de största ultrahögfrekvenstaggarna kan idag lagra 2kB. Det är dock värt att komma ihåg att ju mer data det är som ska läsas, desto längre tid tar det [22].

Hansen och Gillert skriver om fyra olika minnestyper [22]:

#### Enbits endast läsbara

De allra enklaste taggarna lagrar bara en bit, och innehåller inte ens något chip. Dessa kan inte unikt skiljas från varandra och används som varularm i butiker. Taggen fästs på varan och när kunden betalar tas taggen bort eller dödas. Om taggen lämnas kvar på varan kommer det att larma när kunden går ut genom de uppsatta bågarna vid affärens utgång.

#### Endast läsbara med unik identifierare

Dessa taggar har lagrat en unik identifieringssekvens på sitt minnesutrymme vid tillverkningen. Taggarna kan därför användas som unika identifierare och fästas vid föremål som behöver märkas. De är kostnadseffektiva då de är billiga att tillverka och kan återanvändas många gånger.

#### WORM - skrivbar en gång, sen endast läsbara

Dessa taggar kan programmeras med innehåll en gång av användaren, därefter är det endast möjligt att läsa av innehållet. Denna typ av taggar används därför när ett serienummer eller liknande ska utgöra informationen på taggen.

#### Läs-/skrivbar

Taggar som både är läs- och skrivbara är mycket användbara, då de kan kryptera den information som taggen innehåller. För att få åtkomst till innehållet i taggen måste läsaren först verifiera att den har rättigheter till informationen.

### 2.4 Olika typer av taggar

Utöver skillnader i frekvensområde kan ytterligare en uppdelning göras mellan taggar i passiva, aktiva och semipassiva, med skilda egenskaper och användningsområden.

### Passiva taggar

Passiva taggar har ingen egen strömkälla. När radiovågor från läsare når chipets antenn omvandlar antennen energin till elektricitet som kan starta upp mikrochipet i taggen. Taggen har då möjlighet att skicka tillbaka den lagrade informationen. Beroende på hur mycket minne taggen har kostar de från 1 SEK [7].

### Aktiva taggar

Aktiva taggar har en egen strömkälla som används för att driva komponenten och skicka signaler. Dessa taggar skickar information till läsaren, i motsats till passiva taggar som reflekterar tillbaka den efterfrågade informationen. Aktiva taggar kan läsas på upp till 100 meters avstånd, men är i förhållande till de passiva väldigt dyra. Vanligtvis kostar en sådan tagg mer än 150 SEK [6].

### Semipassiva taggar

Semipassiva taggar har, liksom aktiva taggar, också en egen strömkälla, men denna strömkälla används inte för att skicka ut signaler, utan används för att driva mikrochipets krets. Vissa semipassiva taggar kan vara vilande tills de blir "väckta" av en signal från läsaren. Semipassiva taggar kostar från 10 SEK och uppåt [7].

## 2.5 Användningsområden

RFID är en teknik som blir allt vanligare, och har ett brett användningsområde inom identifikation. Bara fantasin sätter begränsningar för hur tekniken kan utnyttjas.

Taggarna med en längre räckvidd har länge använts i stor utsträckning för identifikation inom en rad områden, såsom på containrar vid lossning från fartyg samt i bilar som passerar vägtullar. På kortare avstånd används det även i bland annat husdjur, pass, biblioteksböcker, på Vasaloppsåkare [8] och som stöldskydd. Ett annat stort användningsområde är passerkort, lägenhetsnycklar och elektroniska resebevis. Det är även möjligt att nyttja tekniken vid krypterad identifikation, varpå taggen skickar chiffertext till läsaren, som sen bearbetar informationen [9].

Kreativiteten inom teknikområdet är stor och nya möjligheter till tillämpning identifieras i rask takt. År 2010 års vinnare i designtävlingen *Red Dot Design Award* [10] i kategorin *Design Concept* designade ett boardingkort med en inbyggd kompass, som med hjälp av RFID-tekniken kan visa vägen till rätt gate på flygplatsen.

I framtiden kommer det kanske med hjälp av RFID vara möjligt att korta ner kassaköer i affärer genom att kunderna bara kör igenom sin kundvagn genom en ”lästunnel” som läser av alla taggarna och sen räknar ut det totala priset. De tekniska svårigheter som finns och lättheten att manipulera dessa taggar gör att det kommer ta ett tag innan denna teknik börjar användas [13]. Det genomförs också tester på att märka hemprodukter med taggar så att de kan hjälpa med olika sysslor, såsom att tvättmaskinen varnar om det finns en röd socka i den annars vita tvätten, eller att kylskåpet kan säga till om någon av produkterna i den börjar bli gammal och bör kastas [13].

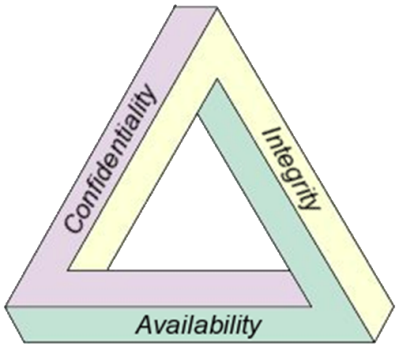
# 3 Säkerhetsproblem

En rad olika säkerhetsproblem är kopplade till RFID-tekniken. Med utgångspunkt från den inom datasäkerhet vanligt förekommande CIA-triangeln, som står för *Confidentiality*, *Integrity* och *Availability*, är det möjligt att identifiera flertalet brister. Avsaknad av väsentliga kontroller och kryptering ökar riskerna i systemet. Se figur 3.

Något som förstärker säkerhetsproblemet ytterligare, är att det ännu inte finns något standardiserat protokoll för dataöverföring som används i större utsträckning. EPC *Electronic Product Code* är ett första försök till en standardisering. Det var ett projekt som hade sin utgångspunkt på MIT i samverkan med ett stort antal globala företag [28].

Tanken med RFID-taggarna är att de ska vara billiga, vilket i sin tur har lett till att säkerhetsfrågan har kommit i skymundan. Säkrare taggar kostar mer, en kostnad som många i dagsläget inte är villiga att betala [12].

Nedan följer korta beskrivningar om de olika säkerhetsproblemen, och avsnittet avslutas med en genomgång av hur ett protokoll fungerar.




Figur 3: CIA-triangeln. Källa: [30]

## 3.1 Avsaknad av autentisering

RFID-system använder sig inte i någon större utsträckning av autentiseringsmetoder. Om en tagg kommer i närheten av en läsare som är av samma typ blir den avläst och lämnar ifrån sig sin information. Den utsätts därmed för vissa säkerhetsrisker. Det är till exempel lätt att kopiera dessa taggar. Genom att istället ha ett schema med ”rullande kod” eller *challenge response* är det möjligt att skapa ett skydd mot förfalskning genom enkel kloning. Rullande kod innebär att taggens information ändras efter varje läsning [11]

och challenge response innebär att läsaren skickar en fråga där taggen kan skapa ett svar med hjälp av en delad hemlighet. Eftersom dessa metoder kräver mer komplicerad elektronik, med högre strömförbrukning som följd, blir dessa taggar dyrare att tillverka.

Med hjälp av en *Relay attack* behöver taggen inte ens kopieras. Någon obehörig läser av innehållet på exempelvis en nyckel från en person som är ute och promenerar, och skickar informationen vidare till någon som står redo vid personens dörr som därmed går upp.

Det är även möjligt att manipulera innehållet i en tagg om den är läs- och skrivbar, genom att ändra eller att förstöra det. En annan möjlig attack är en så kallad *Man in the middle-attack*, där läsaren och taggen tror att de pratar med varandra, medan de i själva verket kommunicerar genom en tjuvlyssnare.

Också läsare kan utsättas för attacker när ordentlig autentisering saknas, såsom exempelvis *DoS-attacker*[3]. I en DoS-attack får läsaren så mycket information tillsänt sig, att den inte klarar av att hantera riktiga förfrågningar längre. Systemet blir alltså oanvändbart.

## 3.2 Avsaknad av kryptering

För att få ett skydd mot att icke auktoriserade läsare kan få ut information från en sändning kan kryptering användas. Få RFID-system använder sig av kryptering, varför det oftast är lätt att avlyssna kommunikationen mellan en läsare och tagg. Med hjälp av ytterligare en läsare i närheten kan all information fångas upp. Det är på så sätt möjligt att exempelvis få reda på vilken information en tagg skickar för att öppna en dörr. Detta är möjligt eftersom kommunikationen sker helt i klartext.

Att kryptering inte används mer utbrett utgör därmed ett stort säkerhetsproblem. Kryptering kräver fler logiska grindar och större lagringsutrymme på taggen, vilket fördyrar integreringen av kryptering. Lagringsutrymmet på en tagg är väldigt begränsat, de billigaste taggarna har bara mellan 64 och 128 bitars ROM minne, där den unika identifieraren lagras [13].

## 3.3 Protokoll

Ett kommunikationsprotokoll är ett sätt att organisera hur kommunikationen mellan läsaren och taggen ska fungera. Daniel M. Dobkin tar i *The RF*

[3]DoS står för Denial of Service.

*in RFID* upp tre faktorer som ett RFID-protokoll behöver definiera [24]:

| | |
|---|---|
| *Radiogränssnitt* | Hur snabbt det går, vilken typ av signal taggen skickar, vilken frekvens som används och hur läsaren definierar en logisk etta och nolla. |
| *Mediumtillgång* | Vem/vilka som får prata när och hur kollisioner hanteras. |
| *Datadefinition* | Vilken sorts data som skickas. |

Det finns ett stort utbud av olika protokoll, som använder sig av olika sätt att hantera dessa tre faktorer, men det är viktigt att taggen och läsaren använder sig av samma definitioner. Mer ingående förklaring kring hur kommunikationen sker på de olika lagren följer under avsnitt 5.5 och 5.6.

De olika frekvensomfången använder sig av olika metoder för kodning - definition av logiskt ett och noll - och för modulation. Dobkin redogör kort för dessa i *The RF in RFID* [25]. Lågfrekvens-RFID använder ofta *frequency-shift keying*, en frekvensmodulering där informationen skickas genom diskreta frekvensförändringar av bärvågens frekvens [27]. Högfrekvens-RFID använder sig istället ofta av amplitudmodulering, där en modulator varierar bärvågens amplitud utifrån meddelandesignalen. Även ultrahögfrekvens-RFID använder sig oftast av amplitudmodulering.

Olika protokoll använder sig också av skilda sätt att hantera paketstrukturer. Denna hantering är ofta inkompatibel mellan olika protokoll, men grundstrukturen är vanligen synkronisering — meddelandehuvud — kommandon — data, oavsett protokoll. Det är vanligt att en enkel felhanteringskontroll görs med hjälp av *Cyclic Redundancy Check*, CRC, där en kontrollsumma för datasträngen först beräknas och sedan efter överföringen kontrolleras och jämförs [25].

# 4 Integritetsproblem

Integritetsfrågan är det andra stora problemet som finns vid användning av RFID-teknologi. Frågan om integritetsbegreppet ämnar belysa problematiken kring att personlig information kan läcka ut eller sparas utan din vetskap, och utan en egen möjlighet att påverka det.

Många personer som använder sig av RFID-tekniken, som vi har pratat med, är inte ens medvetna om att de gör det. Portnycklar, tvättstugebokningsbrickor och passerkort används utan närmare reflektion kring hur de fungerar. Att information om inpasseringar sparas i loggar hos fastighetsförvaltare eller organisationer är oftast inte heller känt av de som använder taggarna.

Något som förvärrar integritetsfrågan är att taggarna kan vara väl dolda, kan spåras och att de har en lång livstid. Genom att sätta upp egna läsare i nära anslutning till redan befintliga, eller genom att få tillgång till den loggade informationen, skulle det vara möjligt att kartlägga en användares vanor och i viss utsträckning även hur denne rör sig.

Nedan redogörs för tre olika aspekter av integritetsproblem som kan uppstå.

## 4.1 Loggningsproblem

Precis som med alla elektroniska system kan användandet av taggen loggas. De spår som RFID-taggarna lämnar efter sig kan sparas i loggar och därmed utnyttjas för att ta reda på var en person eller en vara befinner sig [11]. Om loggarna är omfattande kan det möjliggöra en kartläggning över hur en persons vanor och rörelsemönster ser ut. Det är därför väldigt viktigt att loggarna förvaras säkert och inte sparas under lång tid i onödan.

## 4.2 Informationsläckor

Som beskrivits ovan under säkerhetsproblemen kan en taggs information lätt läsas eller avlyssnas. Detta kan leda till att känslig information kommer ut. Till exempel kan taggar som sitter på läkemedel läcka information om den person som fått läkemedlet utskrivet, såsom vilken sjukdom denna har. Denna information kan i sin tur vara av intresse för såväl försäkringsbolag som arbetsgivare. Ett mindre allvarligt exempel är att någon obehörig skulle kunna se vilka biblioteksböcker en person bär runt på i sin väska.

Dock innehåller taggarna oftast inga stora mängder data, utan den identifierare som finns på taggen kopplas till en databas, där identifieraren matchas till rätt information som bara de som har tillgång till databasen kan se. Detta system liknar det för streckkoder.

### 4.3 Spårbarhetsproblem

Spårbarhetsfrågan är mer komplex. Även om en tagg bara sänder en identifierare kan informationen användas för att spåra ett objekt i tid och rum. Om denna tagg då finns hos en person blir spårningen av ett objekt genast spårning av en människa. Ytterligare en aspekt att väga in är att en person ofta innehar flera olika taggar, och därmed lättare kan råka få sitt liv kartlagt av någon obehörig.

I dagsläget är det inget stort problem med att personer blir kartlagda utifrån sitt RFID-användande, men i takt med att området utvecklas och växer ökar också riskerna. Läsavståndet på de passiva lågfrekvenstaggar som vanligtvis används är kort, vilket försvårar att någon obehörig kan läsa av en tagg utan personens vetskap. Däremot är skyddet obefintligt gentemot någon obehörig som kommer över en större uppsättning loggfiler från RFID-användning. Därigenom är det möjligt att analysera data och spåra personer.

# 5 Lösningar på säkerhets- och integritetsproblem

Det finns en del föreslagna lösningar av varierande kvalitet när det kommer till olika säkerhets- och integritetsaspekter kring RFID-teknologin. Under avsnittet kring säkerhetsproblem föreslogs ett par. Här beskrivs ytterligare ett antal olika metoder som är kopplade till att försvåra möjligheten för obehöriga att tillgodogöra sig informationen från en tagg.

Nedan föreslås fyra lösningar på säkerhets- och integritetsproblemen, alla med sina för- och nackdelar. Därefter beskrivs kopplingen mellan en taggs spårbarhet och taggen och läsarens uppbyggnad.

## 5.1 Minska läsavståndet

En metod är att om läsavståndet för en tagg kortas ned, minskar också chansen för att någon ska ”tjuvlyssna” på läsningen, trots att kryptering saknas. Detta är dock ingen hållbar lösning, då den endast begränsar problemet och inte avskaffar det helt [13].

## 5.2 Döda taggen

Kill the tag är en effektiv metod för att undvika att obehöriga kan spåra användandet av en tagg, men med den stora nackdelen att taggen inte kan användas mer än en gång. Metoden fungerar så att taggen har en *nullfunktion* som aktiveras efter till exempel ett varuköp så att varan inte kan spåras till kunden [18]. En nullfunktion är en funktion som inte returnerar några värden tillbaka när den anropas, och som lämnar programmets tillstånd oförändrat. Taggen beter sig alltså som om den vore död.

## 5.3 Hindra taggen från att höra frågan

Att blockera signalen från läsaren så att taggen inte hör den kan göras genom att stänga in taggen i en *Faradaybur*. Faradays bur är ett utrymme som med hjälp av elektrisk ledande material har avskärmats från elektromagnetiska fält. Taggen stängs alltså in i en metall som inte kan släppa igenom radiosignaler, och på så sätt hindras taggen från att kommunicera med läsaren. Detta är en dyr lösning som inte går att tillämpa inom alla användningsområden. Den skulle passa i till exempel pass eftersom de ändå måste öppnas för att kontrolleras [17], men fungerar inte vid märkning av djur.

## 5.4 Hindra läsaren från att förstå svaret

I den här metoden används exempelvis en *blocker tag*, som förhindrar läsaren från att avgöra vilka taggar som finns i närheten genom att själv skicka ut falska signaler. En blocker tag använder sig i princip av *tree walking*-protokollet och simulerar med hjälp av det ett fullt spektrum med möjliga taggar. Hos en läsare innebär tree walking-protokollet att läsaren ska undvika kollisioner genom att sortera ut en tagg i taget. Den frågar först efter alla taggar som börjar på 1 eller 0. Om fler än en svarar fortsätter den att fråga efter 01, därefter 010 och så vidare, tills bara en svarar [29].

## 5.5 Koppling mellan spårbarhet och lager

En RFID-tagg och -läsares kommunikation byggs upp av tre lager som innehåller olika funktioner och säkerhetsaspekter. De tre lagren är applikationslagret, kommunikationslagret och det fysiska lagret.

### Applikationslagret

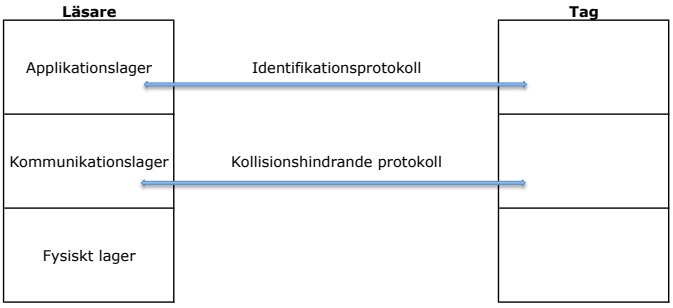
Hanterar information som definieras av användaren. Det kan vara information om det taggade objektet, till exempel en boktitel, eller en identifierare som tillåter läsaren att hämta information i en databas.

### Kommunikationslagret

Definierar hur läsare och tagg kommunicerar. Här finns ett kollisionsprotokoll som sållar ut den rätta taggen att läsa.

### Det fysiska lagret

Definierar det fysiska gränssnittet: frekvensen, datakodning med mera.




Figur 4: De olika lagren

## 5.6 Säkerhetsaspekter i de olika lagren

De tre säkerhetsaspekterna från CIA-triangeln, sekretess, integritet och tillgänglighet, ska säkerställas genom att rätt protokoll implementeras i rätt lager. Gällande integritetsaspekten spårbarhet är det mer komplicerat, eftersom varje lager kan ge ifrån sig information som kan användas för spårning. Därför är det viktigt att se till att även spårning omöjliggörs i alla lager. Dock har de flesta protokoll som används i dagsläget inte tagit alla lager i åtanke för att skapa en säker tagg som inte går att spåra. I figur 4 visualiseras de olika lagren med koppling till olika typer av protokoll.

### Applikationslagret

Applikationslagret är det lager som i dagsläget är det mest utforskade och studerade. För att öka säkerheten nyttjar några av de protokoll som används idag sig av metoden att uppdatera informationen mellan två olika läsningar. Vanligtvis sker detta genom att läsaren förser taggen med det nästa värde som den ska skicka, eller så sänds data som ger taggen möjlighet att utföra en sådan uppdatering själv. Dessa protokoll kan definieras utifrån om läsaren är med i processen eller inte.

Ohkubo har i *RFID Privacy Issues and Technical Challanges* föreslagit ett RFID-protokoll som har visat sig vara säkert, där taggen kan uppdatera sig själv med användning av två *hashfunktioner* [18]. Läsaren behöver alltså inte vara inblandad.

Om läsaren är med i uppdateringsprocessen skickar den tillbaka information till taggen, med ett värde som ska vara omöjlig att särskilja från ett slumpvärde. Det är även viktigt att det värdet bara används en gång. Många av de befintliga protokollen brister i en av eller bägge aspekterna. Det visar hur svårt det är att skapa protokoll som är icke spårbara för taggar som är beroende av att läsaren genererar nya identifikatorer [13].

### Kommunikationslagret

I RFID-system uppstår det kollisioner när en läsare skickar ut en förfrågan om läsning och alla taggar inom räckvidden försöker svara samtidigt. För att undvika detta används ett kollisionsundvikande protokoll. Då taggarna inte har möjlighet att kommunicera med varandra, eller har tillräckligt med kraft för att själva inneha protokollet, faller detta på läsaren. Läsaren måste alltså själv hantera krockarna utan hjälp av taggarna.

Vanligtvis sker detta genom att läsaren frågar alla taggarna efter deras identifikator för att sedan kunna göra en kollisionsfri förfrågan efter en viss tagg som matchar den efterfrågade.

Förr var det vanligast att de protokoll som användes i RFID-system för att undvika kollisioner var egendesignade och inte var öppen källkod, vilket gör det svårt att hitta information om dem. Dock kommer det mer och mer standarder för dessa protokoll, som håller på att fasa ut de egendesignade protokollen. Protokollet väljs till stor del beroende på vilken frekvens som används i RFID-systemet.

Det finns två huvudgrupper av kollisionsundvikande protokoll, deterministiska protokoll och probabilistiska protokoll. De deterministiska protokollen förlitar sig på att alla taggar har en unik identifierare, och att identifieraren förblir oförändrad till slutet av processen. De probabilistiska protokollen är vanligtvis baserade på ett protokoll som heter *Aloha*. I *Aloha* delas kommunikationen upp i ett slumpmässigt antal olika tidsluckor, taggen väljer slumpvis en av dessa luckor och svarar läsaren först när den tidsluckan kommer. Om antalet tidsluckor är färre än antalet taggar uppstår en kollision. För att komma åt den missade informationen undersöker läsaren taggarna en gång till, denna gång kan läsaren tysta de taggar som inte skapat kollisioner, och välja ett mer passande antal tidsluckor för att läsa de kolliderande taggarna [13].

Ett annat exempel på ett kollisionshanterande protokoll är det tidigare nämnda Tree walking-protokollet, som är deterministiskt.

### Fysiska lagret

De fysiska signalerna mellan en tagg och en läsare möjliggör igenkännande av den tagg eller de taggar som blir avlästa, oaktat om den information som kommuniceras kan förstås eller ej. Det kan vara igenkänning av till exempel den frekvens eller kodning av data som används. Även om spårbarheten förebyggs i de högre lagren, kommer det inte ha någon effekt om den inte förebyggs även i det fysiska lagret.

Det största problemet med det fysiska lagret är att det inte finns någon standard för hur radiosändningarna ska ske (frekvens, tidpunkt med mera), eftersom taggar som använder olika standarder är lättare att särskilja vid en läsning. Detta blir ett problem först då flera taggar läses av samtidigt, inte när en enskild tagg läses.

Om en person bär med sig ett flertal taggar med olika standarder, kommer taggarna vara lättare att urskilja från varandra. För en obehörig som vill spåra en person kan detta underlätta det arbetet. Lösningen på detta problem är att införa en standard för hur radiosändningen ska utföras, men för tillverkarna finns det ingen vinst i detta, där ligger fokus på kostnad och storlek istället.

# 6 Metod och utförande

Studien har bestått av en förberedelsefas, en genomförandefas och en avslutningsfas. Alla faser har bestått av olika typer av arbete; litteraturstudie, insamling av data, sammanställning och diskussion.

## 6.1 Förberedelser

Inledningsvis genomfördes en omfattande litteraturstudie för att inhämta information om funktionalitet och tidigare undersökningar som gjorts om säkerhet och integritet inom RFID-området.

För att praktiskt genomföra experiment angående säkerheten har en läsare för passiva lågfrekvenstaggar, en kopieringsapparat som kopierar innehållet på passiva lågfrekvenstaggar samt ett par extra skrivbara taggar införskaffats. Denna utrustning hittades efter sökningar på internet, och kunde inhandlas för endast 700 SEK. Utrustningen har använts i försök att få ut samt kopiera information från taggar.

Resultatet har sammanställts i den här rapporten med bakgrundsfakta, resultat av de experiment och studier som genomförts samt en avslutande diskussion.

## 6.2 Genomförande av studien

Genomförandet av studien har främst skett genom inhämtande och analys av offentligt tillgänglig information, praktiska experiment samt kontakt med fastighetsförvaltare.

### Diskussion kring säkerhet och integritet

Efter att ha läst tidigare rapporter kring ämnena säkerhet och integritet inom RFID-området har det i denna rapport resulterat i en genomgång av dessa frågor samt presentationer av olika lösningar.

### Kopiering av nyckelbrickor

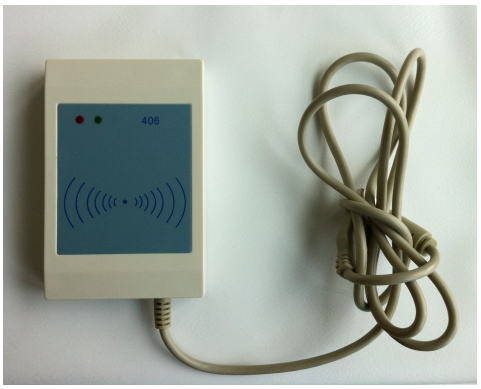
Som beskrivits tidigare är de enkla passiva taggarna de som är billigast att inhandla samt mest lätthanterliga. För den funktionalitet som krävs för nycklar anses de passiva taggarna vara fullt tillräckliga och används därför i stor utsträckning till detta ändamål. Med hjälp av kopieringsutrustningen genomfördes kopiering av ett antal olika passiva taggar som fungerar som nyckelbrickor. Kopieringsapparaten, som drivs av vanliga batterier och sätts på med en liten strömbrytare, är väldigt lättanvänd. Allt som krävs är två

knapptryck. Först läggs brickan som ska kopieras på apparaten, varpå innehållet läses av. Därefter läggs en skrivbar tagg på. Brickorna måste vara i direkt kontakt med apparaten vid kopieringen. Se figur 5.


Figur 5: Kopieringsapparat för 125kHz-taggar

### Inhämtande av information från nyckelbrickor

Med hjälp av RFID-läsaren inhämtades den information som ligger lagrad i nyckelbrickorna. Läsaren kopplas in till en PC med Windows XP eller tidigare genom en USB-port, och fungerar som ett tangentbord som skriver tecken i en textredigerare när en nyckelbricka läggs mot läsaren. Ingen programvara behöver installeras. Genom att läsa av flera nycklar från samma fastigheter, och nycklar från olika fastigheter men hos samma fastighetsägare, gjordes en mindre kartläggning av nycklarnas ID:n. Se figur 6.



Figur 6: Läsare för 125kHz-taggar

### Kontakt med fastighetsförvaltare

När inhämtande av information samt kopiering av nyckelbrickor hade genomförts kontaktades tre av Stockholms större fastighetsförvaltare. Denna kontakt resulterade i att endast en förvaltare svarade, och vi kunde då presentera vad vår studie resulterat i och få svar på några av våra frågor.

## 6.3 Material

Det material som använts för att genomföra de experiment som förekommer i studien är följande.

En RFID-läsare för 125 kHz-taggar, $29.77
`http://www.dealextreme.com/p/pc-usb-125khz-rfid-card-reader-read-only-29278`

En RFID-kopierare för 125 kHz-taggar, $66.14
`http://www.dealextreme.com/p/125khz-rfid-card-copier-duplicator-with-writable-rfid-card-and-keychain-standalone-operation-17230`

Tre extra programmerbara 125 kHz-taggar, $4.65 * 3
`http://www.dealextreme.com/p/125khz-programmable-writable-rfid-keychain-17277`

Alla dessa instrument fanns att finna på hemsidan `dealextreme.com` och var billiga med tanke på vad de sedan kunde ge för information för att föra studien framåt.

# 7 Resultat från praktiska experiment

Detta avsnitt ämnar redovisa de resultat som studien har genererat gällande de praktiska experiment som har genomförts i form av kopiering av nyckelbrickor, inhämtande av information från nyckelbrickor samt kontakt med fastighetsägare.

## 7.1 Resultat av kopiering av nyckelbrickor

Då vi köpte in en kopieringsapparat som kommunicerar på frekvensen 125kHz var det endast sådana taggar vi kunde kopiera. Resultatet av kopieringen var positivt. Vi lyckades kopiera alla port- och lägenhetsnycklar som vi kom över, och det gick bra att öppna de dörrar vars nycklar vi kopierat. Att det var så enkelt att kopiera nycklar var oväntat och förvånande. Kopieringen tog ett par sekunder och allt som krävdes var två knapptryckningar på kopieringsapparaten.

## 7.2 Resultat av inhämtad information från nyckelbrickor

De ID-nummer som vi lyckades avläsa från de taggar som vi hade tillgång till visade sig tillhöra samma nummerserie i samma fastigheter. Däremot såg vi inget mönster inom samma fastighetsägare och olika bostadsområden. På grund av integritets- och säkerhetsskäl har vi valt att inte presentera de ID-nummer som vi läst av. Nyckelbrickorna som avlästes var för få till antalet för att det skulle vara möjligt att genomföra någon mer omfattande kartläggning.

## 7.3 Resultat av kontakt med fastighetsägare

Vi sökte kontakt med ett 20-tal fastighetsskötare och informationsansvariga inom tre större fastighetsförvaltare för studentbostäder i Stockholm, för att informera om att vi lyckats kopiera deras nycklar samt för att ställa frågor till dem. Vi fick ingen respons efter första försöket, men efter upprepade försök fick vi svar från en fastighetsskötare hos en av förvaltarna. Det resulterade i ett möte på fastighetsskötarens kontor, där vi demonstrerade hur nyckelkopieringen gick till, samt fick svar på ett par av våra frågor.

De reagerade först skeptiskt mot vår upptäckt och ville veta mer om vår studie och kartläggning. Deras fokus låg på den kopieringsapparat som vi införskaffat, eftersom de verkade vara medvetna om att kopiering var möjlig, men trodde att det krävdes mer tekniskt kunnande för att genomföra det, inte att det gick med en billig apparat som finns att beställa på Internet.

De personer vi träffade var en fastighetstekniker och fastighetsskötaren samt lite kort två personer till från förvaltningskontoret. Fastighetsteknikern var skeptiskt inställd till att enbart använda RFID-tekniken till lägenhetsnycklar, och tog upp att nyckelanvändningen skulle bli säkrare om den kombinerades med användandet av koddosan som sitter på alla dörrar. Det skulle dock med stor sannolikhet öka kostnaderna för fastighetsförvaltaren när jourpersonal måste rycka ut för att låsa upp dörrar där koden har glömts bort.

Fastighetsteknikern berättade även att alla in- och utpasseringar sparas i loggar. Dessa loggar administreras av en inhyrd IT-lösning, liksom alla ID-nummer till nyckelbrickorna.

Vårt besök hos fastighetsförvaltaren resulterade en vecka senare i ett brev till alla boende i fastigheten där det står:

*Det har kommit till vår kännedom att man med ganska enkla och billiga medel kan kopiera taggar/nyckelbrickor som används i elektroniska passagesystem. Förvara alltid din nyckelbricka säkert och gör den svåråtkomlig när du rör dig ute på stan.*

*Vi har omedelbart satt igång arbetet med att förbättra säkerheten i husets passersystem så vi är steget före bovarna. Vi återkommer med ytterligare information när vi vet mer.*

*Stort tack till Emma Angermund och Emma Lindqvist från KTH som gjort oss uppmärksamma på detta.*

# 8 Diskussion

RFID-tekniken har vuxit snabbt och dess användningsområden ökar hela tiden. Nackdelen med denna snabba tillväxt är att säkerhets- och integritetsaspekterna i utvecklingen har åsidosatts, och istället för att fokusera på att göra tekniken säkrare ligger fokus på att producera mindre, billigare, snabbare och högre presterande taggar och läsare.

## 8.1 Säkerhetsaspekten

Vår studie har visat att det är väldigt lätt att kopiera taggar med hjälp av förhållandevis billig utrustning som finns lätt tillgänglig att köpa på internet. Det faktum att vi lyckades kopiera en lägenhetsnyckel till en studentlägenhet med endast två knapptryck visar att RFID-tekniken används utan närmare tanke på säkerhet. Smidigheten i att använda RFID-tekniken har många gånger fått gå före överäganden runt säkerhetsbrister som finns.

Att använda sig av de enklare modellerna av taggar, som endast kan lagra kraftigt begränsad information utan kryptering, är det billigaste alternativet. Vi anser att de som väljer att använda sig av RFID mer noggrant även bör överväga säkerhetsaspekten. De kan kombinera användandet av taggarna med en sifferkodkombination, eller använda sig av de mer avancerade taggarna som kan utnyttja olika krypteringstekniker. Att inte tänka efter i förväg kan bli kostsamt längre fram.

Att taggar som används som lägenhetsnycklar, tvättstugenycklar eller portnycklar är så lätta att kopiera är något som den vanliga hyresgästen förmodligen inte vet om. Och det finns inte någon som vill att det genom två knapptryck ska gå att kopiera nyckeln in till deras hem. Detta blir även en försäkringsfråga som säkert skulle intressera de försäkringsbolag som försäkrar hem som använder taggar som nycklar, och även fastigheter som använder taggar som portnycklar.

Det är även problematiskt att det är samma nummerserie på nycklarna i ett bostadshus, eftersom det gör det lättare att gissa sig till riktiga nyckel-ID-nummer. Dessa nummer skulle man sedan kunna programmera in på andra taggar för att på så sätt ta sig in i bostäder. Fastighetsförvaltarna bör därför i större utsträckning använda sig av slumpgeneratorer när de programmerar nyckel-ID:n.

Ytterligare en metod för att försvåra möjligheten att gissa sig till fungerande nyckel-ID-nummer skulle vara att lägga in en spärr i läsaren, som gör att om det blir för många felaktiga läsningar på rad under en viss

tid, spärras läsaren under en stund framöver. Det skulle försvåra försök att knäcka ID-nummer genom *brute force*[4].

## 8.2 Integritetsaspekten

Det andra stora problemet med RFID-tekniken är de integritetsproblem som den utökade användningen har skapat. Det går att i stor utsträckning spåra en människas aktiviteter genom att läsa av de taggar som den personen bär med sig. Varor och livsmedel som inhandlas kan vara märkta med taggar, användningen av taggar i olika typer av nycklar och passerkort och märkning av husdjur, alla dessa taggar läses av om de kommer i närheten av en läsare, även om det inte är den läsaren som taggen matchar med. Om denna information läggs ihop går det att spåra en persons vardagsrutiner, till exempel, var personen jobbar, var kläd- och matinköp görs, hur resmönstret med kollektivtrafiken ser ut, vilket träningsanläggningar som nyttjas och var bostaden ligger. I många fall vet användarna inte ens om att de bär runt på olika taggar, eller att de som äger taggarna kanske registrerar varenda gång de används.

Att användandet av elektroniska och identifieringssystem loggas är inget nytt. Informationen sparas oftast lokalt i respektive värddators databas. Det som är speciellt med RFID-tekniken är just att en person kan ha flera taggar som blir avlästa av en annan läsare än de är avsedda för. Den felaktiga läsaren kan logga även dessa åtkomster, vilket är negativt ur ett integritetsperspektiv.

Det allvarliga med loggning av information är att den kan användas på fel sätt. Till exempel skulle en arbetsgivare, som använder sig av taggar för att öppna dörren till kontoret, kunna logga de anställdas arbetstider genom att se när de kommer på morgonen och hur lång lunch de tar. Det är lätt att denna teknik blir ett övervakningsverktyg.

I dagsläget där många användare inte vet att de använder RFID-taggar, än mindre att deras användning kan sparas, saknas det kritiska tänkandet och ifrågasättandet mot användandets utbredning. Om fler skulle vara medvetna om hur tekniken fungerar och vad det finns för brister i den skulle det skapa en debatt angående om dessa taggar ska användas överhuvudtaget, och vad som kan göras för att öka säkerheten i den användning som redan finns.

[4]En metod för att hitta rätt kombination genom att prova många gissningar.

## 8.3 Felkällor

De källor som vi nyttjat under studiens gång har i stor utsträckning varit några år gamla. Många av källorna har varit från 2005 och är alltså inte så pass uppdaterade som vi önskat att de skulle vara. Detta påverkar självklart resultatet av vår studie. Trots detta har vi försökt hitta källor av mer uppdaterad art, men det har tyvärr inte gått så bra.

Andra felkällor som vi stött på är det faktum att de flesta större källor som vi hittat, så som större avhandlingar eller böcker, refererar till varandra. Det verkar vara ett tiotal personer som aktivt skriver om RFID och dessa personer refererar sina verk till varandra, så kallad peer review.

## 8.4 Slutsatser

Studien har visat på ett flertal säkerhets- och integritetsbrister i RFID-tekniken, vilka i huvudsak tas upp under respektive rubrik i rapporten.

Fokus under säkerhetsdelen har legat på att hitta lösningsförslag på förbättringar för att motverka oönskad avlyssning och kopiering av taggar. Det finns en rad olika metoder att använda sig av. Gemensamt för de flesta är dock att det kostar att öka säkerheten i systemet. När det kommer till de fastighetsägare som väljer att använda sig av RFID-teknik i sina nyckelsystem anser vi att det på sikt förmodligen skulle löna sig att ta den högre kostnaden vid inskaffandet, för att slippa obehagliga överraskningar i framtiden. Det är betydligt mer kostsamt att behöva uppgradera systemet i efterhand.

Det är positivt att den generella användningen av RFID verkar vara på väg mot alltmer standardiserade protokoll där säkerheten har fått större uppmärksamhet.

Det är värt att ha en större debatt kring integritetsaspekten dels utifrån perspektivet att utbredningen av tekniken ökar, samtidigt som det är relativt lätt att kartlägga en persons vanor utifrån dennes RFID-användning, men också utifrån perspektivet att loggningen av användandet kan användas som ett medel för övervakning. En ökad debatt kring såväl integritets- som säkerhetsfrågor gällande RFID-användningen skulle i sin tur tvinga fram en förbättring i tekniken inom dessa områden. Tillverkarna skulle behöva tänka om och kanske införa en standard för hur radiosändningarna ska göras, nya bättre protokoll skulle utvecklas och helhetstänket mellan alla lagren skulle utökas.

Förslag på förbättringar:

- Att de taggar som används som nycklar i redan befintliga system kombineras med en pinkod
- Att nyinvesteringar i nyckelsystem använder sig av säkrare taggar med kopieringsskydd och kryptering
- Att standardisera protokollen
- Att de som använder sig av RFID-teknologi, till exempel fastighetsförvaltare, företag eller livsmedelsbutiker, genomgår grundligare utbildning i vad tekniken innebär och dess fördelar och brister
- Att information om loggning av användningen av taggar sprids till användarna

Vi ser positivt på en fortsatt användning av RFID-tekniken för identifiering. Så länge säkerhets- och integritetsaspekterna tas med vid framtagandet av nya och utvecklade användningsområden finns det en stor potential. RFID är både relativt billigt och väldigt smidigt att använda. Det handlar framför allt om att fortsätta att utveckla säkerhetsbitarna samt att använda sig av de metoder och tekniker som redan finns.

# 9 Referenser


[1] *The History of RFID Technology*, RFID Journals hemsida
http://www.rfidjournal.com/article/view/1338/1
Besökt 2011-01-28

[2] *Shrouds of Time – The history of RFID*, AIM Inc, 2001
http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf
Besökt 2011-01-30

[3] *The Basics of RFID Technology*, RFID Journals hemsida
http://www.rfidjournal.com/article/view/1337
Besökt 2011-02-04

[4] *Microchip, microID 125 kHz RFID, System Design Guide*, Microchip Technology, 2001
http://ww1.microchip.com/downloads/en/devicedoc/51115f.pdf
Beökt 2011-02-04

[5] *ISO/IEC 18000*, Wikipedia
http://en.wikipedia.org/wiki/ISO/IEC_18000
Besökt 2011-02-20

[6] *Glossary of RFID Terms: A – E*, RFID Journals hemsida
http://www.rfidjournal.com/article/glossary/1
Besökt 2011-02-20

[7] *Glossary of RFID Terms: M – S*, RFID Journals hemsida
http://www.rfidjournal.com/article/glossary/3
Besökt 2011-02.04

[8] L. A. Karlberg, *Rfid-chip ger rätt Vasaloppstid*, NyTeknik, 2006-03-03
http://www.nyteknik.se/nyheter/it_telekom/allmant/article247251.ece
Besökt 2011-01-25

[9] H-W Wang, R-G Lee, C-C Hsiao och G-Y Hsieh,*Active RFID System with Cryptography and Authentication Mechanisms*, Journal of Information Science and Engineering 26, s. 1323-1344, 2010
http://www.iis.sinica.edu.tw/page/jise/2010/201007_11.pdf
Besökt 2011-01-25

[10] *Winner red dot award: design concept 2010*, red dot online: design concept
http://www.red-dot.sg/concept/porfolio/o_e/PD/R099.htm
Besökt 2011-02-04

[11] *RFID*, Wikipedia
http://sv.wikipedia.org/wiki/RFID
Besökt 2011-01-31

[12] RSA cryptographer Ari Juels on RFID, encryption
http://itknowledgeexchange.techtarget.com/security-wire-weekly/tag/rfid-security/
Besökt 2011-03-23

[13] G. Avoine, P. Oeshslin, *RFID Traceability: A Multilayer Problem*
http://lasecwww.epfl.ch/php_code/publications/search.php?ref=AO05b
Besökt 2011-03-30

[14] RFID-läsare för 125 kHz-taggar
http://www.dealextreme.com/p/pc-usb-125khz-rfid-card-reader-read-only-29278
Besökt 2011-01-30

[15] RFID-kopierare för 125 kHz-taggar
http://www.dealextreme.com/p/125khz-rfid-card-copier-duplicator-with-writable-rfid-card-and-keychain-standalone-operation-17230
Besökt 2011-01-30

[16] Extra programmerbara 125 kHz-taggar
http://www.dealextreme.com/p/125khz-programmable-writable-rfid-keychain-17277
Besökt 2011-01-30

[17] C. Huang,*An Overview of RFID Technology, Application, and Security/Privacy Threats and Solutions*, George Mason University, Electrical and Computer Engineering Department
cryptography.gmu.edu/~jkaps/download.php?docid=1287
Besökt 2011-03-30

[18] M. Ohkubo, K. Suzuki & S. Kinoshita, *RFID Privacy Issues and Technical Challanges*, 48, No. 9 Communications of the ACM, 2005
http://portal.acm.org/citation.cfm?id=1082022
Besökt 2011-03-30

[19] *RFID Frequencies Explained*, RFID Alert
http://rfid-alert.com/rfid-frequencies/, 29 september 2010,
Besökt 2011-01-30

[20] *RFID Frequencies*, Scansource
http://www.scansource.eu/es/education.htm?eid=8&elang=en
Besökt 2011-01-30

[21] *Nomenclature of the Frequency and Wavelength Bands Used In Telecommunications*, International Telecommunication Union (ITU)
http://www.itu.int/dms_pubrec/itu-r/rec/v/R-REC-V.431-7-200005-I!!PDF-E.pdf
Besökt 2011-01-30

[22] W-R. Hansen and F. Gillert, *RFID for the Optimization of Business Processes.* John Wiley & Sons Ltd, England, 2008

[23] K. Finkenzeller, *RFID Handbook. Fundamentals and Applications in Contactless Smart Cards and Identification.* 2nd Edition, Giesecke & Devrient GmbH, München, Tyskland, 2003

[24] D.M. Dobkin, *The RF in RFID: physical layer operation of passive UHF tags and readers 4. UHF RFID Protocols*, 2005, reviderad 2009

[25] D.M. Dobkin, *A Radio-Oriented Introduction to RFID—Protocols, Tags and Applications*, 2005, Summit Technical Media

[26] *Is your underwear spying on you?*, Allvoices
http://www.allvoices.com/contributed-news/6396741-is-your-underwear-spying-on-you/image/59973804-rfid-chip
Besökt 2011-04-04

[27] *Frequency-shift keying*, Wikipedia
http://en.wikipedia.org/wiki/Frequency-shift_keying
Besökt 2011-04-04

[28] E. W. Schuster, D. L. Brock and S. J. Allen *Global RFID*
http://www.springerlink.com/content/978-3-540-35654-7#section=267875&page=1&locus=0
Besökt 2011-04-07

[29] *Singulation*, WIkipedia
http://en.wikipedia.org/wiki/Singulation
Besökt 2011-04-10

[30] *CIA-triad*
http://blogs.technet.com/blogfiles/seanearp/WindowsLiveWriter/LayersDefenseinDepthPart1_B11E/CIA_triad.png
Besökt 2011-06-10

# Figurer