Digitala lås
– en introduktion

OFFENTLIGA FASTIGHETER

Offentliga fastigheter

Samarbetet Offentliga fastigheter består av organisationer som förvaltar många av Sveriges offentliga fastigheter. Tillsammans förvaltar vi skolor, myndighetsbyggnader, försvarsfastigheter, sjukhus och fängelser. I vårt nätverk finns en enorm bredd, inte bara av olika slags fastigheter utan också i form av olika slags erfarenheter. För att ta tillvara och utveckla vår breda kompetens har vi gått samman i Offentliga fastigheter.

Vi bedriver gränsöverskridande utvecklingsprojekt som bygger upp och sprider kompetens samt effektiviserar och förbättrar förvaltningen av våra gemensamma fastigheter. Projekten ska vara angelägna och väcka nya tankar. De ska visa på inspirerande exempel och erbjuda praktiska verktyg. Med andra ord projekt som inte bara gynnar oss själva utan också kan hjälpa och vägleda många fler.

Bakom Offentliga fastigheter står Sveriges Kommuner och Regioner, Fortifikationsverket och Samverkansforum genom Statens fastighetsverk och Specialfastigheter.

Mer information hittar du på **www.offentligafastigheter.se**.

Digitala lås
– en introduktion

Digitala lås – en introduktion

ISBN 978-91-7585-893-7
Upplysningar om innehållet Bo Baudin, SKR
Text Staffan Hellberg, PwC
Omslagsillustrationer Christina Jonsson
Foto PwC
Grafisk form ETC Kommunikation
Produktion Advant
Webbplats www.offentligafastigheter.se

Förord

Syftet med den här skriften är att ge en introduktion till digitala lås. Marknaden har utvecklats fort och digitala lås har blivit ett allt intressantare alternativ till traditionella lås. Införandet av digitala lås är dock en fråga som kräver noggranna överväganden och en klar analys av de för- och nackdelar samt kostnader och nyttor som finns. Eftersom införandet av digitala lås innebär ett teknikskifte är det också viktigt att involvera användare och verksamheter i förändringsarbetet.

Projektuppdraget har initierats och finansierats av Offentliga fastigheter, som i sin tur finansieras av bland annat SKR:s FoU-fond för kommunernas fastighetsfrågor respektive SKR:s FoU-fond för regionernas fastighetsfrågor.

Rapporten är författad av Staffan Hellberg, PWC. Bo Baudin, Sveriges Kommuner och Regioner har varit projektledare. Vi vill tacka alla de personer som bidragit med både konkreta underlag till skriften samt värdefulla synpunkter. Utvecklingen av digitala lås fortsätter och vi får säkert anledning att återkomma med nya underlag i frågan.

Stockholm i september 2020

Gunilla Glasare
Avdelningschef

Peter Haglund
Sektionschef

Avdelningen för tillväxt och samhällsbyggnad
Sveriges Kommuner och Regioner

Innehåll

Sammanfattning

Samhället digitaliseras i allt högre utsträckning. Detta leder till att det ständigt utvecklas nya tekniska och digitala lösningar. Ett av de områden som har utvecklats med hjälp av nya tekniska lösningar är området lås. Detta har tidigare endast bestått av traditionella, fysiska lås men innefattar nu en uppsjö av olika tekniker och funktioner som underlättar, effektiviserar och skapar en större säkerhet.

Dessa nya digitaliserade lås kallas med ett samlingsnamn för digitala lås. Digitala lås öppnas eller stängs med en elektronisk signal. En elektrisk motor påverkar mekaniken i låsenheten så att den öppnas eller stängs. Överföringen av signalen kan ske med olika bärare. En bärare kan exempelvis vara ett vanligt kort i kreditkortsformat, så kallade taggar eller en app i en mobiltelefon. På marknaden finns idag många olika varianter från många olika tillverkare.

Idag används digitala lås både i privata hem och på kontor samt i offentliga lokaler. I den offentliga verksamheten är det särskilt i hemtjänsten som det har funnits ett stort behov. Digitala lås har införts i hemtjänstverksamheten i cirka 180 kommuner. Detta är ett sätt att effektivisera verksamheten genom minskad nyckelhantering samtidigt som kostnaderna minskar och miljöbelastningen minskas genom mindre bilkörning.

En vidareutveckling av digitala lås kallas integrerade system. Idag finns bland annat lås- och passagesystem som är integrerade med varandra samt en integrerad lås- och tidsregistrering vilket kan innefatta att medarbetares arbetstid loggas vid användning av nyckelkort. De integrerade systemen utvecklas vidare och för framtiden spås ökad integration där flera fastigheter kan samspela för att underlätta behörighetsadministration samt att de digitala låsen kan kopplas till andra fastighetsspecifika system i syfte att effektivisera administration, driftskostnader och underhåll.

För att underlätta utvecklingen av integrerade system krävs gemensamma standarder. Det pågår arbete med detta på både internationell och nationell nivå. Nationellt drivs arbetet av behov av plattformar för integrerade system. Systemen gör det möjligt att integrera olika datamiljöer för fastighetsförvaltning och drift i ett och samma gränssnitt. Lås och passage är en del som tillsammans med bokning, tilldelning av tillfälliga tidprofiler, betalsystem, övervakning, detektering och annat gör dessa tillämpningar intressanta i framtiden.

Utvecklingen av digitala lås påverkas av både juridiska aspekter och säkerhetsaspekter. Dataskyddsförordningen gäller då digitala lås innefattar en slags databehandling. Vidare ställer försäkringsbolag krav på lås som bör beaktas vid upphandling av digitala lås. Den säkerhetsmässiga aspekten berör de ökade krav som ställs på digitala lås i form av skydd mot intrång. Det är inte en fysisk nyckel som ska skyddas mot stöld utan det handlar istället om ett system som måste skyddas. Det handlar om att säkerställa att alla nivåer säkras, vilket är särskilt kritiskt i integrerade system där alla nivåer och delar påverkar varandra och måste säkras från intrång och attacker.

Digitala lås innebär således både möjligheter och utmaningar. Det krävs en förståelse för vad området innefattar samt vilka lösningar som passar den egna verksamheten bäst. Använda på rätt sätt finns stora möjligheter till effektiviseringar, både vad gäller tid och resurser samt en större säkerhet för verksamheten. Digitala lås kan således ha ett stort värde för verksamheten.

1

Introduktion

Bakgrund

Digitaliseringens tid är här och tillvaron styrs i större omfattning av tekniska lösningar. Medborgarna är vana vid en snabb teknikutveckling och de efterfrågar enklare lösningar för att klara vardagens bestyr. Vi lever i en mer digitaliserad värld där vi ofta är uppkopplade mot ett IT-system via dator eller smartphone. Med en smartphone klarar vi mycket av de dagliga uppgifterna såsom resor, bankärenden, inköp, mediabevakning och sociala möten och kontakter. Tekniken för att använda telefonen för att öppna och stänga dörrar står på gränt.

Alla människor har inte förmåga att ställa om till ny teknik. En del av förändringarna bromsas upp av beprövade fungerande tekniker och traditionella lösningar.

Inom området digitala lås sker en utveckling och det finns exempel på väl fungerande tillämpningar. Området har stor utvecklingspotential och det spås en betydande utveckling när det gäller att integrera digitala lås och passagelösningar med bokningssystem och skapa en miljö där traditionella nycklar inte används. Det kan nämnas att cirka 180 kommuner har infört digitala lås i hemtjänsten.

Traditionella lås har utvecklats över lång tid och de är robusta och har en lång livslängd innan de blir utslitna och behöver bytas ut. Det förutspås att dessa lås har tillämpningar en lång tid framöver.

Oavsett tekniska lösningar eller graden av ny teknik kvarstår behoven att förhindra och försvåra inbrott eller intrång för att skydda värden såsom människor, materiella tillgångar, informationstillgångar, varumärken och förtroende.

Vidare är även utrymning en aktivitet som skapar behov av lösningar kopplat till lås och passage. Vid händelse av brand finns omfattande krav på en säker och snabb utrymning, men utrymning kan även krävas vid andra typer av händelser. Inom vissa verksamheter ställs krav på att människor snabbt ska kunna samlas i säkra utrymmen. Det kan vara hot- och våldssituationer eller så kallade skolattacker. Denna ”inrymning” syftar till att

skydda människor mot pågående fysiskt våld. Härvid förutsätts tekniska och digitala lösningar för att detektera händelser och snabbt larma, öppna eller låsa dörrmiljöer. Lås- och passagelösningar ska således inte endast fungera för att stänga ute obehöriga, de ska även vara utformade för att möjliggöra ut- och inrymning vid behov.

Målgruppen för denna skrift är beslutsfattare och personer som jobbar inom något område där lås och passagesystem påverkar verksamheten. Det kan till exempel vara fastigheter och byggnader, boende, uthyrning, säkerhet, drift och underhåll samt hemtjänst och annan kommunal service. Syftet med skriften är att öka kunskapen om digitala lås och hur nya tekniker blir ett inslag i upphandling samt hur digitala lås kan implementeras och utgöra ett värde för verksamheten.

2

Definitioner

Vad är digitala lås?

Digitala lås betyder att låset öppnas eller stängs med en elektronisk signal. En elektrisk motor påverkar mekaniken i låsenheten så att den öppnas eller stängs. Elektroniken kräver tillgång till ström, ett batteri eller nätspänning som är transformerad till svagström. Överföringen av signalen för att öppna eller stänga ett lås kan ske med olika bärare. En bärare kan vara ett vanligt kort i kreditkortsformat eller så kallade taggar. En bärare kan också vara en mobiltelefon med en app eller programvara som är standardiserad och med hög säkerhetsnivå. Bäraren har olika nivåer av säkerhet och kan vara krypterad med hög säkerhetsklass.

I ett beröringsfritt system sker överföringen av en signal för öppning utan direkt kontakt mellan bärare och läsare. Det är vanligt att verifiering av signalen sker vid ett avstånd upp till 10 cm. Nya tekniker finns och oftast innebär de att bäraren finns i en smartphone där verifiering kan ske på avstånd på ett antal meter. Det räcker med att personen närmar sig läsaren för att dörren ska låsas upp. Detta kan medföra en osäkerhet om rätt person passerar igenom dörren. Vidare finns även magnetläsare där bäraren (magnetkortet) ska dras igenom en springa.

Det finns många olika definitioner av digitalt lås. En allmän beskrivning som oftast används är att låset är digitalt då det inte krävs en fysisk nyckel. Många förknippar även digitala lås med låsenheter som administreras tillsammans i ett system där behörigheter tilldelas och där spårbarhet kan finnas för passager. Detta benämns passagesystem.

Utöver detta finns det system på marknaden som består av en blandning av en traditionell fysisk nyckel och en digital verifiering för att kunna öppna låset. Dessa system har en hög säkerhetsnivå och kräver inte tillgång till ström.

Digitalt lås

Fysiska lås

Fysiska lås är de ”traditionella” låsen med en nyckel som förs in i en låscylinder vid öppning och stängning. En låsenhet består av en låscylinder, ett låshus, ett slutbleck samt eventuella förstärkningsbehör. Det förekommer många olika system på marknaden. Även de så kallade tillhållarlåsen och hänglås med nyckel tillhör kategorin fysiska lås.

Fysiska lås är fortfarande den vanligaste låsmiljön i fastigheter, bostadsmiljöer och flerfamiljsboenden. En hyresvärd som tillhandahåller lås till boende och lokaler har ofta ett nyckelsystem med olika serier av nycklar såsom huvudnyckel, nycklar till utrymmen för drift och underhåll samt gemensamma lokaler. I systemet finns också nycklar som enbart fungerar i separata dörrar till lägenheter och motsvarande.

Fysiskt lås

Elektromekaniska lås

Elektromekaniska lås eller elektriska lås är fysiska lås där låsen öppnas och stängs med hjälp av en motor eller magnet. Systemen kräver tillgång till svagström. Elektromekaniska lås kan vara elslutbleck eller motorlås.

Elslutbleck underlättar snabb passage och är den produkt som är vanligast inom elektrisk låsning. Elslutblecket kan vara konstruerat så att dörren är låst eller olåst i strömlöst läge. Olika typer av elslutbleck används till exempel för enklare intern låsning under dagtid i offentliga fastigheter, kontor, handel och i gemensamma utrymmen inom bostadssektorn. Systemet uppfyller höga krav på många passager, utrymning och brythållfasthet.

Motorlås är lås med motorstyrd regel och har en mycket högre säkerhetsnivå än elslutbleck. Låsets regel styrs vanligen med en motor via en styrenhet vid såväl upplåsning som låsning. Motorlås används primärt inom offentliga fastigheter, kontor, industri och handel som natt- eller skalskyddslåsning när lokalerna inte är bemannade.

I system som baseras på elektriska koder finns dels en läsare, dels en kontrollenhet som utvärderar den lästa koden. Den elektriska koden läses i läsaren, utvärderas i kontrollenheten som därefter ger en styrsignal till låsets elektriskt styrda slutbleck (elslutbleck) eller motordrivna regel (motorlås).

Dessa typer av låssystem finns i olika slags passagelösningar med flertalet dörrmiljöer. Se nedan om passagesystem.

Elektromekansikt lås

Passagesystem

Ett passagesystem är ett tekniskt system med ett flertal elektromekaniska lås, bärare av kod, läsare och styrsystem för att verifiera behörighet samt enheter för administration av systemet.

För öppning av en dörr krävs en passagebricka eller annan bärare (något man har) och/eller en kod (något man kan). Det kan också finnas system med biometrisk information (något man är) såsom ansiktsigenkänning, ögonskanner eller fingertoppsavläsning. För en ökad säkerhetsnivå kan flera av dessa kombineras.

I de flesta passagesystem används idag kort eller nyckelbrickor som elektroniska nycklar. Nyckelbrickorna har många namn som tagg eller kort.

Den största skillnaden jämfört med ett traditionellt låssystem är att systemet loggar användandet. Det blir fullt spårbart och i efterhand går det att kontrollera vem som passerat den aktuella dörren och när detta skedde. Administratören kan koppla olika tidszoner till dörren så att passage endast kan ske vid vissa tider. Likaså kan administratören enkelt spärra kort som förkommit.

Moderna inpasseringssystem har en högre säkerhetsnivå och det finns tekniker som har en mycket hög skyddsnivå. Det kan fortfarande

förekomma system med bristfällig säkerhetsnivå och kort som är möjliga att kopiera. Kort eller motsvarande bör kombineras med en PIN-kod för ökad säkerhetsnivå. Risken för att en obehörig person ska göra intrång reduceras då betydligt.

Exempel på bärare och avläsningstekniker

Det förekommer många olika slags bärare och tekniker för överföring av signal för att verifiera en användare och ge tillträde till ett utrymme. Det kan vara:

- Beröringsfritt med "taggar", chip eller smartcard (till exempel NFC, RFID eller MIFARE)
- Digitala nycklar (en kombination av fysisk nyckel med elektroniskt id)
- Mobila nycklar (NFC eller Bluetooth Low Energy)
- Magnetkort
- Fingeravtryck
- Biometriska tekniker

För att överföra och tolka signaler används olika tekniker och standarder. Ett vanligt sätt att överföra signal är med radiovågor inom olika frekvensområden. Teknikerna har utvecklats över tid och har bland annat skiftande säkerhetsnivåer och olika möjligheter till kryptering.

RFID betyder Radio Frequency IDentification och är en överföringsteknik med stöd av radiovågor. Den finns som passiv där taggen får tillräckligt mycket ström från läsaren och som aktiv där taggen har en egen strömkälla. RFID har full spårbarhet och är vanlig som tillträdesapplikation.

EM betyder Electromarine och är en RFID-teknik och en standard som används i många passagesystem. EM-tekniken har ett läsavstånd på upp till 20 cm beroende på miljö, läsare och antenn. Ett EM har inte så hög säkerhetsklass och är därför tillämplig i redan säkrade miljöer.

MIFARE är en snabbt växande standard inom RFID-tekniken. Mifaretekniken är beröringsfri och ofta används ett smartcard. På korten kan information lagras vilket möjliggör mer omfattande kryptering. På detta sätt kan säkerhetsnivån öka och tillämpning blir möjlig i miljöer med högre krav på säkerhet. Det förekommer olika versioner av MIFARE. Först ut var MIFARE Classic och därefter utvecklades MIFARE Plus. Efterföljare och komplement till dessa standarder är MIFARE DESFire. MIFARE Plus och MIFARE DESFire har en längre nummerserie för de unika chipnumren. MIFARE Plus är utrustad med en 128-bitars AES-kryptering.

NFC betyder Near Field Communication, (närfältskommunikation på svenska). NFC är en radiobaserad överföringsmetod för kontaktlöst utbyte av data över korta sträckor. Räckvidden sträcker sig upptill 10 cm. Det korta avståndet gör det svårt att avlyssna. Tekniken finns för applikationer på plastkort men också för mobiltelefonen. En mobiltelefon med inbyggt NFC kan användas för att öppna dörrar.

BLE, Bluetooth Low Energy är en annan teknik som använder mobiltelefon som bärare.

Tillämpningsområden

I nyinstallationer används Mifare främst för mer avancerade företagsinstallationer. I enklare företagsinstallationer och bostadsfastigheter är EM, Electromarine-standarden den absolut vanligaste. Säkerheten mellan bäraren och läsaren beror uteslutande på den teknik man väljer och man kan förenklat säga att magnetkort är det minst säkra och beröringsfri krypterad teknik som exempelvis Mifare är betydligt säkrare. De okrypterade Electromarinstandarderna kan läsas av på distans även om nyckeln ligger i en ficka.

Gemensamt för beröringsfria tekniker är att de är svårare att sabotera och enklare att skydda.

Så kallade taggar kan se ut som ett litet batteri på en plastbit och kräver elektronisk kontakt mellan nyckel och läsare.

Biometriska tekniker har under lång tid setts som hi-tech-lösningar. Det har uppkommit flera biometriska enklare lösningar, men i och med introduktionen av GDPR, (The General Data Protection Regulation) och det faktum att biometriska uppgifter anses särskilt känsliga har biometri inte slagit igenom i Sverige och flera av de biometriska lösningar som satts upp tidigare har nedmonterats.

I många passagesystem saknas grundläggande funktioner som koppling till Microsoft AD, personalkatalog eller katalogtjänster för att automatiskt hantera när en person avslutar sin anställning och behörigheterna i passagesystemet ska upphöra. Det kan också vara komplext att hantera olika passagesystem i samma organisation då inloggningar, benämningar, klientfunktioner, datamodell och tolkning av kort skiljer mellan olika fabrikat. Det saknas dessutom standarder för systemen. I och med detta växer det fram en marknad för överordnade system där organisationens samtliga passagesystem kan hanteras på samma sätt.

Krypteringstekniker och system

En överföringsteknik i en bärare kan förses med olika former av kryptering för att uppnå en önskad grad av säkerhet. Kryptering har gamla anor och i början användes enklare manuella metoder som var relativt enkla att knäcka. För passagesystem och digitala lås är krypteringen elektronisk och bygger på avancerade matematiska beräkningsmodeller, så kallade algoritmer. En kryptering består av två delar. Den första är en algoritm och den andra är en krypteringsnyckel. Vid kryptering omvandlas data till en annan form av data och både sändare och mottagare har samma algoritm och krypteringsnyckel. Det finns olika krypteringsmetoder och de skiljer sig åt i fråga om säkerhet och hastighet. För att öppna dörrar krävs system som möjliggör hög hastighet då öppningssignalen måste komma snabbt. Krypteringsnyckelns längd är avgörande för säkerhetsnivån och ju längre nyckel som används, ju längre tid tar det att knäcka den. En 128-bitars kryptering är näst intill omöjlig att knäcka. I dagsläget förekommer olika nivåer av krypteringar och det är först på senare tid som säkerhetsnivån har ökat.

Integrerade system

Det talas om integrerade system och även här tolkas definitionen olika. Nedan ges några exempel på tillämpningar.

Lås och Larm

Inom kontor och handel är det inte ovanligt att lås (passage) och larmsystem är sammankopplade. Avlarmning sker när bäraren (passagekort, tagg eller mobiltelefon) presenteras vid läsaren och verifierar användaren som behörig att passera.

Larm kan aktiveras manuellt när sista personen lämnar lokalen. Larmsystemet kan också kopplas på automatiskt, en viss tid efter att ingen detektering skett eller vid en förutbestämd tid. Finns personal kvar i lokalen förvarnas dessa genom en ljud- eller ljussignal innan larmet kopplas på. Vid högre krav på skyddsnivå låses den så kallade nattlåsningen vid tillkoppling av larmet.

Brandutrymning ska alltid kunna ske när det finns personal kvar i utrymmen och olika tekniska lösningar ska sammankopplas för att säkerställa en säker och snabb utrymning.

Lås och tidbokning

I flerfamiljshus förekommer det flera lösningar där bokning av tid för tvättstuga sker digitalt via en centralt belägen display i fastigheten eller via fjärrinloggning med mobiltelefon eller dator. Dörren till tvättstugan är bara möjlig att passera i anslutning till bekräftad tvättid. För dörröppning används oftast ett kort eller tagg. Detta system minskar riskerna för tillgrepp och störningar i tvättstugan. Spårbarheten ökar och analys av beläggning och användande kan göras för utveckling, service och underhåll.

För kommunal verksamhet eller motsvarande, som ger medborgare tillgång till idrottshallar eller annan service, kan bokning med fördel göras digitalt och behörighet tilldelas enbart under begränsad tid. Tillträde och inpassering kan ske enbart under den tid då bokning är bekräftad. Inga nycklar behöver hämtas av brukaren och risken att nycklar förkommer eller inte lämnas tillbaka elimineras. Vi kan räkna med att appar till smartphones utvecklas så att dörrar kan öppnas med mobiltelefonen genom nya överföringstekniker.

Lås och arbetstid (hemtjänsten med mera)

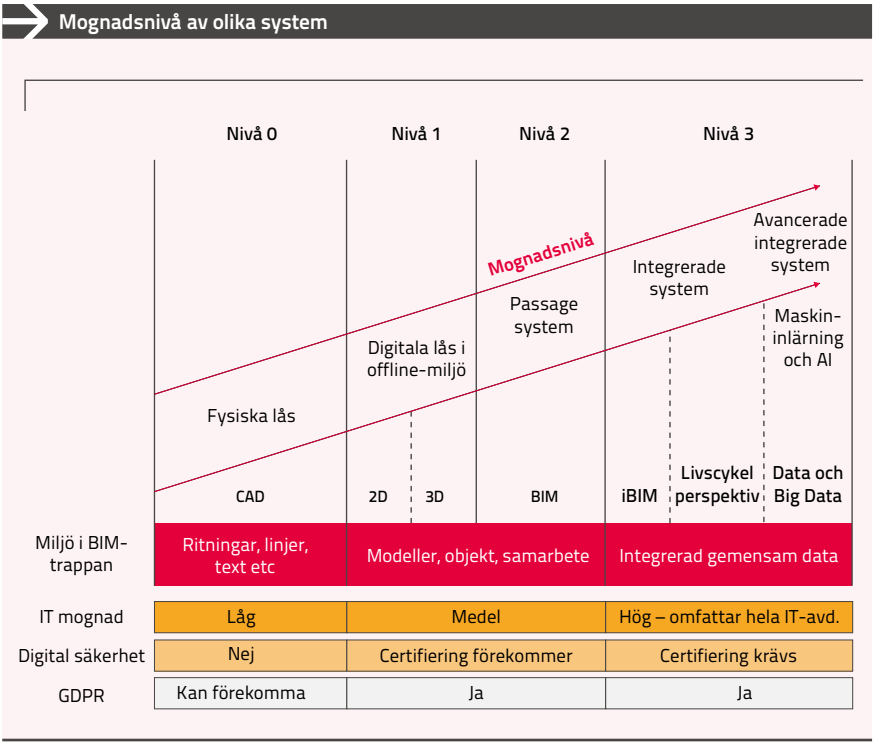
Arbetstid kan registreras eller tid för fakturering kan starta och sluta efter att arbetstagare presenterat sin elektroniska nyckel vid läsaren. Tidregistrering sker under denna tid och utgör underlag för ersättning både till arbetstagare och för avgift till kund.

Framtida integrerade system

En utveckling sker mot att integrera lås- och passagesystem med andra fastighetsspecifika system i syfte att effektivisera administration, driftskostnader och underhåll. Integration sker mellan lås, affärssystem, medlems- och personalsystem för att administrera tillträden och ekonomisk uppföljning. Plattformarna bygger på så kallade öppna källor och kod för programmering är fri att använda. I en framtida miljö med möjlig integration kan olika låssystem användas tillsammans. Befintliga passagesystem kan länkas samman och utgöra en lösning i ett gemensamt gränssnitt. Integrationen möjliggör också en förenklad, effektivare och säker behörighetsadministration där behörigheter kan tilldelas på distans efter olika krav.

Nedan ges exempel på integrerade system som är under utveckling och en beskrivning av tillämpningsområden samt kort information om tekniska aspekter.

Sammanfattning och mognadsnivå av olika system



FIGUR 1 ▪ Ett urval av förekommande lås- och passagesystem kopplat till den så kallade BIM-trappan. Bilden visar även en bedömning av nivån på IT-mognad, digital säkerhet och dataskyddsförordningen.

3

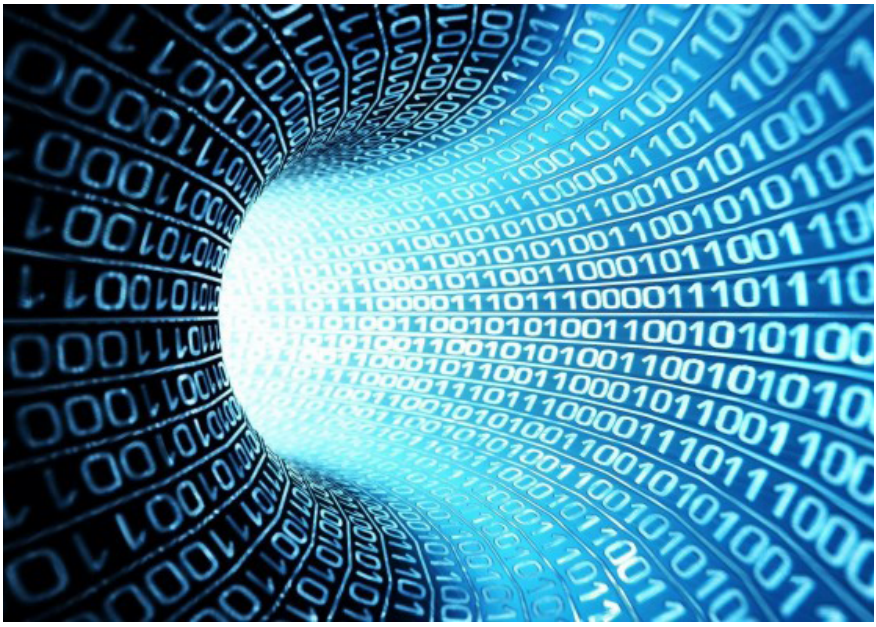
Digitaliseringen och framtiden

I en analog värld finns inget stöd av datorer eller smartphones. I låsets värld används de traditionella fysiska nycklarna. Digitaliseringen pågår för fullt och det talas bland annat om Artificial Intelligence (AI), robotinlärning, simulering, sensorer, Big Data och Internet of Things.

Den globala digitaliseringen innebär att ny teknik förändrar och stöper om samhället i grunden. Vardagen förändras och omfattningen samt takten i förändringen kan vida överstiga vad medborgaren kan ta till sig. Så stort att det nästan inte går att greppa. Företagens tjänster och affärsmodeller förändras, vår kommunikation förändras, vårt sätt att arbeta utmanas och vår vardag förändras.

Regering och riksdag lägger en grund för nationella IT-satsningar samt skapar förutsättningar för en bra infrastruktur för IT och så att den offentliga sektorn kan digitaliseras. Digitaliseringspolitiken handlar om att använda och främja de möjligheter som digitaliseringen för med sig. Området omfattar bland annat reglering av IT och elektronisk kommunikation, liksom nät- och informationssäkerhet, frekvenspolitik och frågor om internets förvaltning. I området ingår också frågor om tillgång till bredband och digital infrastruktur samt frågor om digitalisering och IT inom offentlig förvaltning.

Många människor ser digitaliseringen som ett hot som tar bort arbetstillfällen och fördyrar verksamheter. Andra ser fördelar och att digitaliseringen hjälper och utvecklar samhället. Människan riskerar att förminskas eller glömmas bort i all teknikhets. Digitaliseringen ska ju trots allt vara till gagn för människan och också utföras av människan. Ett hinder för utvecklingen av IT inom offentliga verksamheter sägs vara attityder och kunskapsbrister bland tjänstemän och personal. Genom olika utvecklingsprojekt och satsningar blir digitalisering och IT en mer integrerad del av den offentliga verksamheten. Vårt förhållningssätt till IT är väsentligt och det behövs en kultur som inte bara gillas utan också levs i vardagen.



Digitalisering handlar också om att utveckla verksamhetens processer och system. Man kan skönja mer utveckling mot plattformstänkande som innebär att samla data på ett gemensamt sätt i en gemensam miljö. Öppna och standardiserade gränssnitt skapas och gör det enklare att integrera system och ta hand om gemensam data för att skapa användarvänliga och effektiva system. Digitalisering innebär också ett förändrat förhållningssätt till våra befintliga sätt att arbeta och våra processer. Från känt och förutsägbart till föränderligt och oförutsägbart. Förhållningssätten hos samtliga aktörer utmanar oss.

Ett område som utvecklats inom den kommunala verksamheten är digitalisering av lås inom hemtjänsten. Inom dess verksamhet läggs i dag stora resurser på hantering av nycklar till bostäder. Dagens system med individuella fysiska nycklar kräver att brukare lämnar ut nycklar för att ge hemtjänsten tillträde till bostaden. Genom en övergång till digitala lås skulle en betydande minskning av nyckelhanteringen kunna genomföras och med det finns en stor potential till kostnadsbesparingar, ökad effektivitet inom hemtjänsten och en minskad miljöpåverkan.

4

Är fastighets-branschen redo för digitalisering?

Fastighetsbranschen påverkas av digitaliseringen och verkar i en tid av krav på effektiviseringar och transparens. Effektiviseringar av energiåtgång för el, värme, kyla, ventilation och andra system för fastighetsdrift omformar traditionell förvaltning till nya former av integrerade system för drift och underhåll. Energianalyser görs för att uppnå miljömål och som underlag för effektiviseringar och fastighetsutveckling.

Vid bostadsuthyrning tillhandahåller fastighetsägaren låssystem till bostaden och tillhörande utrymmen. Oftast förekommer låssystem med fysiska nycklar och låssystemet omfattar en mångfald av nycklar och nyckelkombinationer. Ett system av nyckelkombinationer finns för gemensamma utrymmen och rum för drift och underhåll. En så kallad huvudnyckel kan finnas. Huvudnyckeln används med restriktioner och förvaras säkert hos fastighetsägaren. Många fastighetsägare har lämnat systemet med huvudnyckel då det är förknippat med stora problem och kostnader om en huvudnyckel försvinner.

Vid uthyrning av lokaler för kommersiellt bruk eller till andra organisationer sker uthyrning oftast utan att fastighetsägaren tillhandahåller lås. Detta för att behoven av skyddsnivåer samt lås och passagesystem växlar och att hyrestagaren har sina egna krav och system. Dessa omständigheter uppmanar inte fastighetsägaren till att införa gemensamma och integrerade låssystem för sina fastigheter.

Inom kommunal verksamhet ska vissa lokaler vara tillgängliga för medborgarna. Servicen till medborgaren kräver att utlämning av fysiska nycklar görs för att få tillgång till idrottshallen eller annan typ av lokal. Servicen medför ofta en omfattande administration. Risken för att nycklar tappas bort eller inte lämnas åter i tid gör systemen sårbara. I detta sammanhang passar ett digitalt låssystem bra.

Standardisering underlättar fastighetsförvaltning

För att lyckas med att skapa säkra integrerade system krävs ett omfattande arbete med att utveckla plattformar som möjliggör hantering av data från olika källor och att paketera dessa i användarvänliga gränssnitt. För lås och passage ställs höga krav på säkerhet, och att dessa system blir omöjliga att ”hacka” och komma igenom, i syfte att skydda värden och tillgångar samt skapa tillförlitlighet i systemen.

Under en relativt lång tid har fastighetsbolag använt dataprogram som till exempel CAD och BIM samt olika system för driftövervakning. Nu är tiden mogen för och det pågår en utveckling mot integrerade fastighetssystem.

Fastighetsbranschen har inte varit så bra på att samordna olika tekniker och standarder och det finns många vertikala system. Men allteftersom fler digitala tjänster och mer teknik gör sitt intåg i fastigheterna ökar behovet av att allt kan kommunicera med det fastighetssystem som används. Fastighetssystemen måste även kunna prata med varandra så att det blir möjligt att med bibehållen information byta system. Att tvinga systemleverantörerna att göra speciallösningar för varje kund och delsystem skulle vara en mycket opraktisk lösning.

Internationellt pågår ett utvecklingsarbete för att svara upp mot de behov som finns identifierade samt att möta innovationer som inte helt kan förutses idag. Det finns olika slags plattformar och de stora aktörerna inom data utvecklar globala system som har tillämpningar i Sverige.

Nationellt pågår arbete som drivs av behov av plattformar för integrerade system. Nedan redovisas fyra exempel på system som är i drift och under utveckling. Systemen gör det möjligt att integrera olika datamiljöer för fastighetsförvaltning och drift i ett och samma gränssnitt. Lås och passage är en del som tillsammans med bokning, tilldelning av tillfälliga tidprofiler, betalsystem, övervakning, detektering och annat gör dessa tilllämpningar intressanta i framtiden.

Sveriges Allmännytta

Sveriges Allmännyttas digitaliseringsråd initierade hösten 2019 Digitaliseringsinitiativet, som syftar till att förstärka och accelerera medlemsbolagens digitalisering.

Digitaliseringsinitiativets roll är att leda, samordna och driva processen framåt och för att uppnå målet om konkret förändring inom allmännyttan avser man bygga Allmännyttans digitala plattform.

Inom ramen för projektets pågående omvärldsbevakning och behovsanalys utreds bland annat det omfattade utvecklingsarbete som Sveriges Allmännytta hittills genomfört tillsammans med BIM Alliance, i förhållande till den målarkitektur som ska tas fram och ligga till grund för den nya gemensamma digitala plattformen.

Initiativet är en treårig satsning som drivs i projektform och ett år in i satsningen har ett hundratal av medlemsbolagen anslutit sig.

Sveriges Allmännytta har, sedan tidigare, i samarbete med BIM Alliance arbetat fram nya gränssnitt som gör det möjligt för fastighetsförvaltningssystem och lås- och passagesystem att kommunicera inbördes och med varandra. Det gemensamma standardiseringsarbetet har fått stor betydelse för fastighetsbolagen och innebär även att BIM, (Building Information Modeling) etableras starkare inom förvaltningsområdet. Gränssnitten bygger på fi2xml och är öppna och fria att använda. Fi2xml kan ses som ett gemensamt språk, ett gränssnitt som gör det möjligt att läsa information från olika databaser.

Bland målen finns att minska miljöpåverkan och energiförbrukning samt att förbättra service och information till hyresgästerna. Även ökad trygghet och bättre möjligheter för äldre att bo kvar så länge som möjligt i sin lägenhet finns bland målen.

Arbetet startade med framtagning av ett API för fastighetssystem. API är ett gränssnitt som gör det möjligt för olika programvaror att prata med varandra. Syftet var att uppfinna så lite som möjligt själv och istället använda befintlig standard. Allt arbete med att utveckla standarden fi2xml var en starkt bidragande orsak till att projektet kunde starta. API:et bygger helt på fi2xml och på REST-teknologi, det vill säga hur man ställer webbaserade frågor och hur svaret i sin tur returneras. Projektet skulle inte utveckla ett API för fastighetsbranschen utan huvuduppgiften var att se till att fi2xml används på rätt sätt. En annan uppgift för BIM Alliance har varit att utveckla programmeringsverktyget fi2express där alla fi2-objekten finns tillgängliga i olika programmeringsmiljöer. De som utvecklar applikationer behöver

inte längre tänka så mycket på fi2xml, det sköter verktyget om, och därmed kan utvecklingstiden minska till en tredjedel. Att utveckla fi2express så att allt som används i API:et finns med där är en viktig del av arbetet.

När det standardiserade gränssnittet för informationsutbyte för fastighetssystem är utvecklat är det dags för systemleverantörerna att bygga in detta i sina system. Därefter ska BIM Alliance certifiera att systemen uppfyller kraven på BoIT API:erna. I samband med uppgraderingar och när nya system ska köpas in kommer certifieringarna att efterfrågas i form av skall-krav.

Den färdiga lösningen gör det möjligt för beställarsidan att konkurrensutsätta systemleverantörerna, båda när det gäller själva systemen och moduler till dessa, som till exempel lås, men vi öppnar även upp för en marknad med delade tjänster, molntjänster, som inte är hårdintegrerade hos systemleverantörerna. Det blir lättare att byta ut ett fastighetssystem mot ett annat eftersom allt är standardiserat. Bedömningen är att API-arbetet kan få fart på utvecklingen av tredjepartsprodukter samt att de som idag är systemleverantörer och har bra moduler till sina system kan sälja dessa även till kunder som använder andra fastighetssystem.

Arbetet med att utveckla ett API för lås- och passagesystem har pågått under en längre tid. Digitala låssystem används än så länge mest till allmänna utrymmen men antalet digitala lås till lägenhetsdörrar ökar stadigt. Låsen måste kunna fungera med olika fastighetssystem och därför är behovet av en standard stort, inte minst med tanke på att lagen om offentlig upphandling kan medföra att ett fastighetsbolag plötsligt kan ställas inför en helt ny låstillverkare.

Det skulle bli mycket problematiskt om inte de olika delarna kan prata med varandra och med systemen. Dessutom vill man kunna konkurrensutsätta låstillverkarna fullt ut. Efter arbetet med API för lås- och passagesystem fortsätter arbetet med individuell mätning av energiförbrukning, det vill säga att utveckla API för sensorer och mätare av olika slag som ska kunna kommunicera med de olika fastighetssystemen. Samtliga API som tas fram finansieras av Sveriges Allmännytta, bygger på fi2xml och är öppna och tillgängliga för alla.

Certifieringen av fastighetssystem är genomfört likaväl som certifieringen av ett lås- och passagesystem. Tillverkarna av dessa system ligger långt framme med att integrera API:et i sina lås eftersom behoven av samordning är stora. Husen blir allt mer komplexa och innehåller allt mer teknik så behovet av BIM växer. Arbetet med API:er är till nytta för hela branschen.

Real Estate Core

Real Estate Core är ett gemensamt digitalt fastighetsspråk som bygger på så kallad Open Source-teknik. Systemet lanserades i juni 2018 och syftar till att få kontroll över alla data som genereras i en byggnad. Real Estate Core är framtaget i samarbete mellan Vasakronan, Akademiska Hus, Willhem, Klipsk AB, Rise och Jönköping University.

Information kan hanteras och överföras mellan olika fastigheter och data kan tolkas på ett enhetligt sätt.

Det finns i dag många olika standarder och system i byggnader. Real Estate Core är ingen ny standard, utan förhåller sig till de standarder som redan finns och binder samman BIM, styr- och regler och IoT, (Internet of Things). Olika delar benämns på samma sätt och efter hur de förhåller sig till varandra. Real Estate Core fokuserar på att slå samman och överbrygga tre huvudområden.

1. Digital information om byggnadens konstruktionselement med mera som bland annat finns i BIM.
2. Kontroll och drift av byggnaden.
3. IoT-teknik.

Det gemensamma digitala språket gör att fastighetsägaren får möjlighet till full kontroll över alla data som genereras i en byggnad. Det gör det lättare både att driftoptimera och energieffektivisera men också att ta fram nya tjänster till hyresgäster och leverantörer samt anpassa sina byggnader till den smarta stadens krav. Real Estate Core är ett bidrag till den smarta staden som bland annat Stockholms stad driver som utvecklingsprojekt.

En gemensam plattform stärker också fastighetsägarens roll som beställare av tekniska tjänster och underlättar i fråga om offentlig upphandling.

Digitala låssystem och befintliga passagesystem kan med lätthet integreras i plattformen. Härvid uppnås effektivisering och enhetlig hantering av behörighetsadministration.

Amido

Företaget Amido utvecklar ett system som benämns Alliera. Systemet integrerar inte samtliga fastighetsspecifika system, utan har fokus på att integrera olika nyckelfria passagesystem i ett helt bestånd av fastigheter oavsett geografisk belägenhet. Systemet bygger på en tekniskt avancerad

plattform som går att kombinera med de flesta förekommande nyckelfria passagesystem. Systemet har ett självdokumenterande och öppet API som tillåter integration av olika funktioner. En sådan typ av paraplyplattform automatiserar hantering av personal och behörigheter. Den interna personalen hanteras genom integration med personaldatabas, i de flesta fall Microsoft Active Directory. När en ny person läggs till i personaldatabasen skapas samma person i systemet med rätt information och behörigheter. Den dagen som anställningen upphör spärras personen, och ett eventuellt glömt kort utgör ingen säkerhetsrisk. Extern personal hanteras genom att ett formulär fylls i på en webbplats, därefter attesterar en behörig person och den som behörigheten ska gälla för registreras i systemet och kan hämta en tagg eller ett kort. Systemet möjliggör också att en app kan laddas ner och programmeras för att öppna dörrar. Tider för behörighet kan varieras utifrån behov och uppdrag. Kommunikation med användare kan ske via sms och e-post. Administration kan skötas centralt eller decentraliserat. En central kundtjänst kan hantera administration och om en kommersiell lokal hyrs ut kan administrationen följa med till hyresgästen.

Om det förekommer dörrmiljöer med fysiska nycklar för utrymmen för drift och underhåll, hemtjänst eller om det av andra skäl finns fysiska lås, kan behörighetsstyrda elektroniska nyckelskåp användas. Ingen service med nyckelutlämning behövs utan systemet håller reda på vem som har hämtat och vem som har vilken nyckel och om den är återlämnad eller inte. Systemet kommunicerar med brukaren och påminner om att lämna tillbaka nyckeln i tid.

Accessy AB

Den svenska branschorganisationen Fastighetsägarna och Fastighetsägarna Stockholms förvaltningsbolag har tillsammans med några av landets fastighetsbolag; Vasakronan, Humlegården, Fagebe, Akademiska hus och Castellum startat bolaget Accessy AB. Genom det gemensamt finansierade bolaget vill grundarna skapa en självständig operatör för utveckling av digitala nycklar.

På sikt hoppas initiativtagarna att fler aktörer ska ansluta sig, så att lösningen kan slå igenom på bred front.

Målsättningen är att med Accessy skapa en digital plattform där fastighetsägare enkelt kan fördela access, rättigheter och behörigheter, till låsta utrymmen som kontor, mötesrum, lokaler eller lägenheter.

Tjänsten ska bland annat hitta lösningar för följande problemområden och skapa möjlighet för:

- En nyckelfri miljö
- Åtkomsträttigheter delas av systemet, som direkt är tillgängligt för slutanvändare
- Identifiering via BankID
- Kostnadseffektiv och lättanvänd enhets- och rättighetshantering
- Återkalla rättigheter om det behövs
- Minskade investerings- och driftkostnader för lås- och nyckelsystem
- En öppen och horisontell lösning för en mängd olika applikationer och system

Inera

Inera är ett aktiebolag som ägs av regioner, kommuner och SKR Företag. Uppdraget är att skapa förutsättningar för att förbättra och effektivisera sina verksamheter, genom att förse ägarna med gemensam digital infrastruktur och arkitektur.

Just nu vidareutvecklar Inera denna infrastruktur, bland annat för att skapa flexiblare och säkrare sätt att logga in i e-tjänster, men också för att underlätta för organisationer att hantera och anpassa sina egna lösningar till en modernare infrastruktur.

Grundläggande i förändringsarbetet är den referensarkitektur för identitet och åtkomst, som Inera tillsammans med flera andra organisationer gemensamt tagit fram.

Identitet och åtkomst syftar till att fastställa vilka användare som kan få tillgång till en organisations informationstillgångar och till vilken grad de får behandla informationen med verksamhetskraven och de regulatoriska krav som verksamheten är förenad med som grund.

Ineras infrastruktur för identitet och åtkomst omfattar ett antal infrastrukturtjänster som hanterar och säkrar behörig åtkomst till information.

I det pågående arbetet med att formulera en strategi för identitet och åtkomst med kommunernas behov i fokus, har ett 50-tal representanter från Sveriges kommuner intervjuats. Det är tydligt att det finns en stark önskan att även autentisering i appar standardiseras och att de befintliga lösningarna i kommunen, för autentisering, används även här.

Digital säkerhet

I en uppkopplad värld ökar riskerna för attacker som kan slå ut hela system och orsaka stora kostnader samt stora driftsproblem.

Ingångarna för en attack kan vara många. Mycket av våra prylar vi har i hemmet, på arbetsplatsen eller på andra platser har en koppling till internet med IoT, (Internet of Things).

För att lyckas med införande av digitala lås och integrerade system förutsätts att kraven på god digital säkerhet och IT-säkerhet är uppfyllda. Det är fråga om tilltro från användarna samt krav i beställning och tillämpning på att värden skyddas i alla led.

Det digitala låset i en hemmiljö måste uppfylla kraven på att inte kunna ”hackas” så att passage kan ske otillbörligen. Likaså måste överföringstekniker och teknik bakom passagelösningar vara säkra mot attacker och systemen måste vara krypterade och motsvara kraven för en godkänd certifiering. Vid integrerade lösningar blir kraven för digital säkerhet för hela IT-systemet påtagliga så att det inte finns några möjliga ”luckor” att hacka sig in i.

Utmaningen finns i att säkra samtliga led från programmeringen av bäraren (plastkortet eller smartphonen) till att passage skett av behörig person. Det krävs en säker kommunikation mellan operatör, produkt, användare och digital pryl samtidigt som det ska ges möjlighet till snabbhet och enkla lösningar. Säkerheten måste hanteras på alla nivåer och led i de lösningar som tas fram.

För att lyckas med en god digital säkerhet finns det ett antal områden som bör beröras. Fem områden kan sägas vara centrala. Det första är klassning av de tekniska komponenterna i system såsom bärare och system för öppna dörrmiljöer, noder och centraler. Det andra är administrativ säkerhet där arbetsflöden och processer, kontroller av personer som administrerar behörighetssystem, själva behörighetssystemet, revisioner och uppfyllnad av behörighetssystemet. Det tredje är den digitala säkerheten i ett integrerat system i en mer komplex IT-miljö där flertalet system är sammankopplade och där kravet på skydd mot dataintrång är stort. Härvid är också kravet på driftssäkerhet i IT-miljön viktigt. Det fjärde området

är det fysiska skyddet av datorhallar för IT-drift av passagesystem. Här ingår larm och övervakning, tillträdesskydd och brand- och sabotageskydd av centraler, kopplingsrum och kabelinstallationer. Det femte och sista området är att skapa en säkerhetsmedveten kultur. Medarbetare och användare av systemen bör ha kunskaper om risker och hot och samtliga bör tänka på och leverera säkerhet.

Standarder och certifieringar finns för allt från ledningssystem till komponenter. Att genomföra revisioner blir viktigt för att säkerställa kravuppfyllnad och hög säkerhet för systemets användning över tid. I takt med att systemen blir mer integrerade bör certifieringar och revisioner bli en självklar del i driften av ett system med lås och passage.

Befintliga standarder och certifieringar som är tillämpliga inkluderar men är inte begränsade till SS-ISO/IEC 27000-serien, ISO/IEC 18000-serien samt Svenska Stöldskyddsföreningen, SSF 1075 utgåva 1, Distribution, lagring och användning av digitala nycklar.

7

Juridiska aspekter på digitala lås

Dataskyddsförordningen (GDPR, The General Data Protection Regulation) gäller i princip för all automatiserad behandling av personuppgifter och i vissa fall även manuell behandling av personuppgifter. Personuppgifter innefattar varje upplysning som avser en identifierad eller identifierbar fysisk person.

Dataskyddsförordningen gäller för personuppgiftsbehandling som har anknytning till EU, antingen när den som behandlar personuppgifterna är etablerad inom EU eller då någon utanför EU erbjuder tjänster och varor till personer inom unionen.

Organisationen

Dataskyddsförordningen gäller i princip inom all slags verksamhet och oavsett vem som utför personuppgiftsbehandlingen. Den gäller således för företag, föreningar, organisationer, myndigheter och privatpersoner. Den som behandlar personuppgifter måste i vissa fall utse ett dataskyddsombud. Ombudets roll är att kontrollera att dataskyddsförordningen (GDPR) följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser.

Digitala lås och passagesystem omfattas av databehandling och GDPR blir tillämplig.

Privatpersonen

All information som handlar om fysiska personer som kan identifieras är personuppgifter. Det spelar ingen roll om personen är direkt identifierbar genom uppgiften, eller om det krävs att ytterligare information inhämtas för att denne ska kunna identifieras. Det kan vara till exempel namn, e-postadress, ett foto på personen, ID-kortnummer och IP-adress när någon surfar på nätet.

Försäkringsbranschen

Försäkringsbolagen, försäkringsbranschen och olika samarbetsorgan såsom Svenska Stöldskyddsföreningen (SSF) har över tid jobbat med krav på fysiska lås, omslutningsytor och andra frågor för att klassificera olika skyddsnivåer och standarder för ett bra inbrottsskydd. I försäkringsavtalet mellan försäkringsgivaren och kunden finns det villkorat krav som försäkringstagaren måste uppfylla för att försäkringen ska vara giltig vid till exempel ett inbrott. Det kan vara kvaliteten och utformningen av lås och tillbehör men också regler som gäller när tillträde ges till bostad genom att tillfällig behörighet delats ut via ett digitalt administrationsverktyg. Regelverket är ”spretigt” och det kan noteras att den digitala utvecklingen ibland går före försäkringsbolagens krav. Det rekommenderas att det inför varje upphandling och installation av digitalt lås görs en samverkan med aktuellt försäkringsbolag för att klargöra villkoren för en gällande försäkring.

Lagen om offentlig upphandling, LoU

Lagen om offentlig upphandling är styrande och i många delar omfattande. I fråga om upphandling av system för lås- och passagesystem kan det krävas att leverantören har erforderliga och godkända certifieringar för att installera och underhålla systemen. Det är endast leverantörer som är godkända av respektive producent som har tillåtelse att sälja, reparera och installera utrustning till ett specifikt system. Varje producent utbildar sina leverantörer och ger endast certifikat till de som genomgått utbildningen med godkänt resultat. Det är möjligt att byta en leverantör i en ny upphandling om de har godkända certifikat. I offentlig upphandling finns det begränsad möjlighet att efterfråga ett specifikt varumärke. Om ett varumärke av olika sakliga skäl måste anges ska ”eller likvärdig produkt” tilläggas. Skyddskrav, villkor från försäkringsbolag och resultat av risk- och sårbarhetsanalyser utgör också krav i upphandlingen.

En så kallad funktionsbaserad offentlig upphandling kan göras då integrerade system finns i drift. En funktion kan då efterfrågas i upphandlingen och bakomvarande lås- eller passagesystem har ingen betydelse då de fungerar i det integrerade systemet. I framtiden då det sannolikt finns många integrerade system utvecklade underlättas processen för offentlig upphandling och då en leverantör kan ta ett helhetsgrepp om systemet kan det kanske också innebära färre leverantörer till en verksamhet.

8

Investeringar, kostnader och nyttor

Att investera i ny teknik är inte sällan förknippat med stora kostnader. Samtidigt är investeringen oftast förknippad med effektiviseringar i arbetsprocesser och ökad användarnytta. Investeringar drivs i många fall av behovet av utveckling och det är inte ovanligt att en verksamhet måste göra investeringar för att tillgodose kravet på att använda ny teknik. Det förekommer att leverantörer slutar supportera och underhålla äldre teknik och system vilket gör en investering nödvändig. I offentlig verksamhet görs nya upphandlingar med jämna tidsintervall och det kan innebära en annan prisbild än tidigare.

Att redovisa kostnader för att installera digitala lås, passagesystem och/eller integrerade lösningar är svårt då många faktorer och omständigheter påverkar kalkylen. En investeringskalkyl bör ta hänsyn till å ena sidan kostnader och å andra sidan intäkter och kostnadsbesparingar. Bland annat kan följande poster ingå:

Kostnads- och utgiftssida

- Upphandlingskostnader
- Installationskostnader
- Administration för drift
- Personalbehov
- Drift, underhåll och service
- Tillkommande kostnader för drift och underhåll av IT-system
- Licenskostnader
- Beräknad livslängd (eventuell avskrivning)
- Kostnader som uppstår i samband med krav på certifieringar och standarder
- Kostnader för krav på revisioner och kontroller av systemen
- Utbildningskostnader

Intäkter och kostnadsbesparingar

- Effektiviseringar av administration
- Besparingar i effektiviseringar av processer
- Minskade kostnader för att hantera fysiska nycklar, huvudnyckelsystem, hantering av förkomna nycklar
- Personalbehov, besparingar som uppkommer då medarbetare kan övergå till annan verksamhet
- Eventuell lägre kostnad för drift och underhåll
- Beräknad livslängd jämfört med aktuellt system
- Beräknad kostnad för att nya användare ska kunna använda systemet

Användarvänlighet och nyttor för medborgare eller kunder är svårt att prissätta men bör ingå i överväganden och beslutsfattande.

9

Från vision till verklighet – en spännande framtid

Digitala lås kommer! Utvecklingen har börjat och det finns bra tillämpningar. Det finns ett stort bestånd av fysiska lås och det finns många fungerande passagesystem med en relativt lång livslängd kvar. Det är inte rimligt att ta dessa ur drift och ersätta med nytt. Utmaningen blir att ta vara på fungerande system och integrera i smarta övergripande lösningar. Det pågår ett omfattande utvecklingsarbete inom digitala lås och produktfloran ökar med mer lättanvända och kostnadseffektiva lösningar. Användarna, människan, tar till sig ny teknik och är van vid att öppna dörrar med passerbricka och/eller en smartphone. Vi kan räkna med att appar i telefoner blir allt vanligare bärare av funktion för att passera in i låsta utrymmen. Offentlig verksamhet har börjat ett gediget arbete med att effektivisera hemtjänsten med tillämpningar av digitala lösningar som sparar tid, kostnader och är miljövänliga. Denna utveckling kommer att fortsätta och kompletteras med fler funktioner för att ytterligare effektivisera verksamheten.

Den digitala säkerheten ökar och den tekniska utvecklingen gör att kraven på hög säkerhetsnivå uppfylls. Det ger användaren hög tilltro till systemen. Standarder och certifieringar ökar och fler protokoll tas fram. Vi kan skönja en ökning av revisioner och kontroller av system i syfte att visa att kravställningen uppfylls. Inom den fysiska säkerheten görs inga avkall och låssystem kommer att anpassas till smarta lösningar som öppnar och stänger med hjälp av en övervakad miljö som detekterar hotfulla och farliga händelser snabbare än en människa klarar. Tekniken hjälper oss.

Med stor sannolikhet kommer vi få se att kommunala och privatägda fastighetsbolag och stora förvaltare kommer att utveckla sina fastighetssystem mot integrerade lösningar. Integrationen av systemen skapas med hjälp av öppna och tillgängliga gränssnitt med ett plattformstänk som gör administration och hantering både tilltalande och lättåtkomlig.

I framtiden kanske en hel stadsmiljö kommer att integreras. Den smarta staden uppstår och tillämpningsområdena är många. Kopplat till digitala lås och säkerhet kan nämnas att räddningstjänsten kan nå fram till platsen för en brand och/eller komma in i boendemiljöer med hjälp av ett integrerat system som öppnar till exempel pollare eller andra väghinder i samband med larm i räddningstjänstens väg. Likaså kan dörrar in till bostadshus, in i lägenheter eller andra lokaler öppnas i förväg så att räddningstjänsten får fri väg och full tillgänglighet.

En öppen fråga är om och när den digitala miljön har öppnats helt och teknikens framsteg tagit sin tribut? Frågan är också hur lång tid detta tar? Två, fem eller fler år?

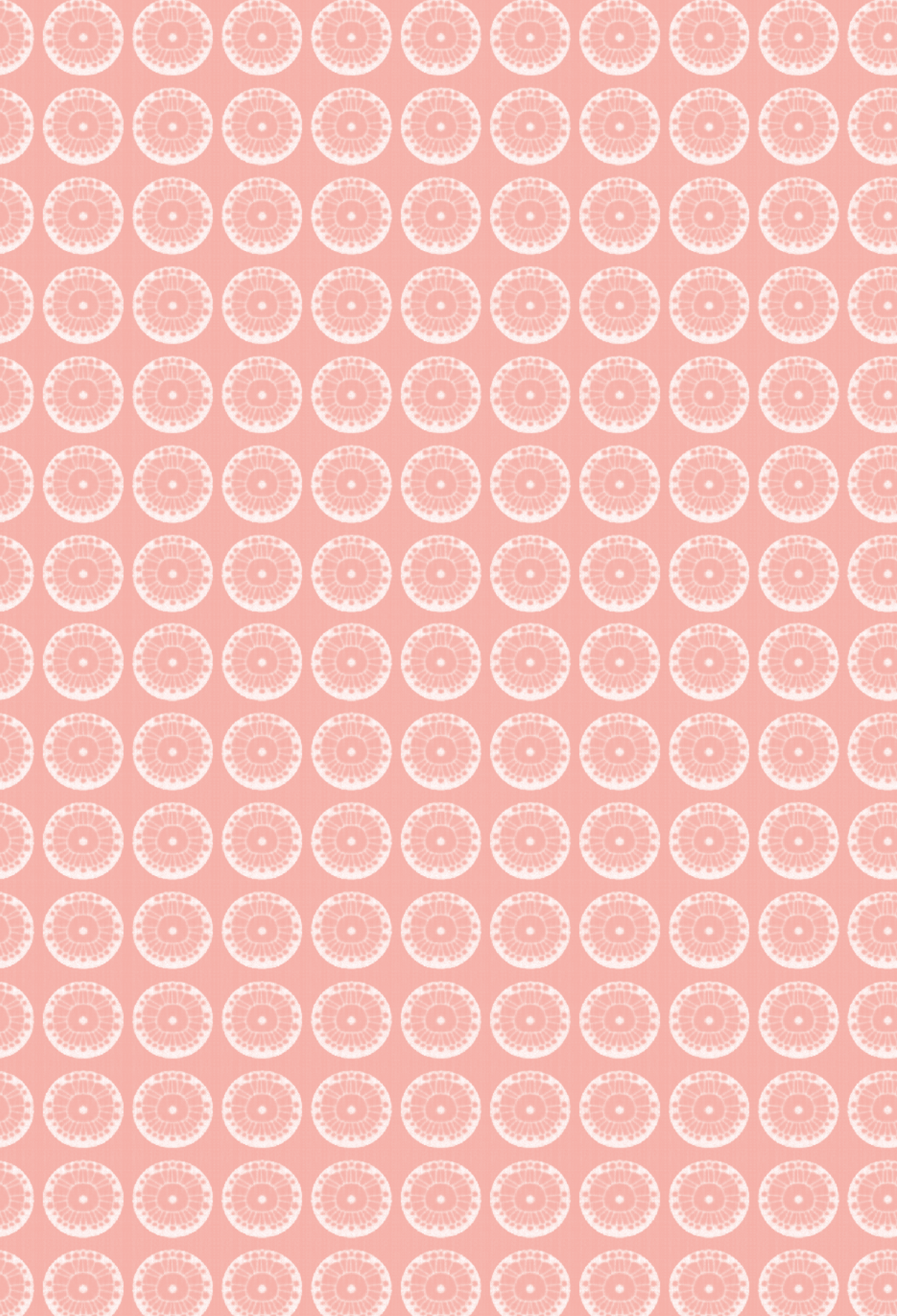
Begreppsförklaring

Begreppsförklaring

Begrepp/förkortning	Innebörd
Accessy	Aktiebolag finansierad av bland annat branschorganisationen Fastighetsägarna samt ett antal fastighetsägare
AI	Artificiell Intelligens. Konstgjord Intelligens se ML nedan
Amido	Aktiebolag som tillhandahåller en plattform för integrerad hantering av digitala nycklar
API	Application Program Interface, är ett gränssnitt som gör det möjligt för olika programvaror att prata med varandra
Big Data	Komplexa och omfattande datamängder som kommer från flera och olika källor
BIM	Building Information Modeling. Informationsflöde och hantering av digitala representationer av fysiska och funktionella egenskaper i byggandet av och i förvaltningen av en fastighet
BIM Alliance	BIM Alliance är en ideell förening som arbetar för bättre samhälls-byggande med hjälp av BIM
Biometriskt	Egenskap hos en människa som kan användas för att öppna något, till exempel med ögonigenkänning, fingeravtryck eller ansiktsigenkänning
BLE	Bluetooth Low Energy, lågeffektsvariant av Bluetooth
Bluetooth	Bluetooth eller Blåtand, en trådlös överföringsteknik mellan elektroniska komponenter
Bärare	Något man har där en kod för att öppna en dörr finns lagrad. Kan vara ett kreditkortsliknande kort, tagg eller en mobiltelefon
CAD	Computer Aided Design. Datorstöd för att ta fram byggnadsritningar
Digital säkerhet	Se IT-säkerhet
Elektromekansikt lås	Lås som öppnas och stängs med hjälp av en motor eller magnet
Elslutbleck	En enklare variant av elektromekaniskt lås där en stålplatta på dörr-karmen har en elektrisk öppningsmekanism
EM	EM som betyder Electromarine är en RFID-teknik och en standard som används i många passagesystem. EM-tekniken har ett läsavstånd på upp till 20 cm beroende på miljö, läsare och antenn
Fysiskt skydd	Mekaniska, tekniska, administrativa och organisatoriska åtgärder som delvis syftar till att skydda en anläggning mot obehörigt intrång, sabotage eller annan påverkan
Förstärkningsbehör	Plåt kring en låsenhet som förstärker inbrottsskyddet
GDPR	The General Data Protection Regulation. Dataskyddsförordningen från 2018 gäller i hela EU och har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter
Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten
Inera	Aktiebolag som samägs av regioner, kommuner och SKR och med uppdrag att skapa förutsättningar för att digitalisera välfärden, genom att förse ägarna med gemensam digital infrastruktur och arkitektur
Informationssäkerhet	Skydd av analog eller digital information utifrån sekretess, riktighet, tillgänglighet och spårbarhet. Inkluderar IT-säkerhet

IT-säkerhet	Att skydda en organisations (företags, myndighets) värdefulla tillgångar som information, maskinvara och programvara. IT-säkerhet koncentrerar sig på hot och skydd förenade med användning av informationsteknik
Kryptering	Text som kodas om genom att på olika sätt kasta om bokstäver (kryptera). Mottagare måste göra samma sak för att texten ska bli läsbar (dekryptera)
LoU	Lagen om offentlig upphandling
Läsare	En mottagare som avläser en kod från ett kort, tagg eller mobiltelefon för att öppna en dörr
Motorlås	Ett lås som öppnar eller stänger med hjälp av en elektrisk motor. Är kraftigare än elslutbleck
ML	Maskininlärning. Ett datorprogram läser in, tolkar data och programmerar automatiskt en ny tillämpning
MIFARE	En RFID-teknik med beröringsfri överföring av data. På korten kan information lagras. MIFARE Classic, första versionen MIFARE Plus, efterföljande version. Kan ha 128-bitars AES-kryptering MIFARE DESFire, komplement till övriga versioner. Har en längre nummerserie för de unika chipnumren
NFC	Near Field Communication, (närfältskommunikation). Är en radiobaserad överföringsmetod för kontaktlöst utbyte av data över korta sträckor
Offline	Utan uppkoppling mot en databas
Omslutningsyta	Lokalens avgränsningar (väggar, tak, golv, dörrar, portar, fönster etcetera) mot andra lokaler i byggnaden samt ut mot det fria
Passagesystem	Ett system av flera elektroniska eller digitala lås som öppnas med smartkort, tagg eller mobiltelefon
Real Estate Core	Ett digitalt språk för att hantera data från olika källor inom BIM, Internet of Things samt styr- och reglerteknik. Publiceras som open source
REST-teknologi	Hur man ställer webbaserade frågor och hur svaret i sin tur returneras
RFID	Radio Frequency IDentification är en överföringsteknik med stöd av radiovågor
Risk	En kombination av sannolikheten för att en händelse ska inträffa och dess konsekvens
Slutbleck	En stålplatta på dörrkarmen som låshuset är monterat på
SS-EN	Svensk Standard – Europanorm. Till exempel SS-EN 1627
SSF	Stöldskyddsföreningen
Sveriges Allmännytta	Bransch- och intresseorganisation för kommunala och privata bostadsföretag
Sårbarhet	Avsaknaden av en eller flera av varandra oberoende skyddsåtgärder och brist i skyddet av en tillgång exponerad för hot. Kan delas in i tre komponenter – Säkerhetsmedvetande (utbildningsnivå, uppträdande, viljan att skydda sig). – Resurser (hårdvara, byggnadstekniska, organisation). – Exponering i tid och rum (när/var tillgången utsätts för hot).
Tillhållarlås	Ett lås utan låscylinder med låsenheten inne i låshuset. Oftast som komplement till ett cylinderlås. Kallas också över-eller underlås
Tillgångar och värden	Allt som är av värde för organisationen

TABELL 1 ▪ Begreppsförklaringar



OFFENTLIGA FASTIGHETER

Digitala lås
– en introduktion

www.offentligafastigheter.se

Digitala lås har finansierats av organisationen Offentliga fastigheter och är en av två fristående skrifter om framtidens lås

ISBN: 978-91-7585-893-7
www.offentligafastigheter.se