This watermark does not appear in the registered version - http://www.clicktoconvert.com

Information om säkerheten i de svenska bankernas nya chipkort

TDDC03, våren 2004

Anna Berglund, annbe187
Åsa Karlsson, asaka100

Handledare: Viiveke Fåk

This watermark does not appear in the registered version - http://www.clicktoconvert.com

Information om säkerheten i de svenska bankernas nya chipkort

Anna Berglund
annbe187@student.liu.se

Åsa Karlsson
asaka100@student.liu.se

Sammanfattning

I denna rapport har vi sökt och utvärderat befintlig information i svenska medier och på svenska banker angående säkerheten i de nya chipkort som just nu håller på att lanseras som bankkort i Sverige. Vi har tittat på vilken kunskap i ämnet som finns på lokala bankkontor. Vi konstaterar att chipkorten innebär en ökad säkerhet då de nya bankkorten i framtiden kommer att vara betydligt svårare att kopiera. Vi kommer fram till att informationen som står att hitta från alla håll angående säkerheten i allmänhet är knapphändig men att detaljerade svar på säkerhetsfrågor går att få om rätt personer nås.

1. Inledning

Svenska banker håller idag på att införa en ny teknik för att öka säkerheten i bankkort. Tidigare har kort som lagrar information i en magnetremsa använts. Nu ska istället information lagras på ett datachip som är inbyggt i kortet. Dessa nya kort kallas chipkort eller smarta kort. Bytet av teknik ska innebära en ökad säkerhet för bankernas kunder. Men vad vet egentligen bankernas kunder om den höjda säkerheten, vilken information finns att hitta?

2. Syfte

Syftet med denna rapport är att undersöka säkerheten i de nya chipkorten samt titta på hur svensk media och svenska banker informerar om säkerheten. Vi undersöker och utvärderar den information som finns att hitta angående den nya tekniken. Vi tittar på vilken kompetens som finns på lokala bankkontor angående säkerheten i de nya chipkorten.

3. Frågeställning

Våra frågeställningar är: Hur är säkerheten i de svenska bankernas nya chipkort? Hur god är informationen om säkerheten i de nya bankkorten? Hur lätt är det att hitta denna information? Vad krävs för bakgrundskunskap för att förstå informationen? Hur stor kunskap angående säkerheten finns på våra lokala bankkontor?

4. Metod

I utformandet av rapporten har vi studerat material angående magnetkort och chipkort. Vi har också tittat på var säkerheten i chipkorten ligger. Material har vi bland annat hämtat ur dagstidningar, tidskrifter, webbsidor och ur informationsblad från banker. De banker vi har tittat på är Nordea samt Föreningssparbanken. Vi har genomfört ett antal telefonintervjuer med personer insatta i projekten att införa chipkort i dessa banker. Vi har också intervjuat bankpersonal på bankernas lokala kontor i Linköping samt på kortservice för att undersöka vilken kompetens som finns angående de nya korten.

5. Magnetkort

Den teknik som idag är vanligast för att lagra information på bankkort är magnetkort. I dessa kort lagras informationen i en magnetremsa på kortets baksida. I remsan, som är gjord av ett ferromagnetiskt material, finns små laddade partiklar. Genom att utsätta dessa för ett yttre magnetfält kan man få dem att byta polarisation, d.v.s. byta plats på dess nordpol och sydpol. Styrkan på magnetfältet som behövs för att åstadkomma detta byte mäts i koercivitet. Ett kort med låg koercivitet kräver ett svagare magnetfällt än ett med hög koercivitet. Detta betyder också att ett kort med låg koercivitet löper större risk att raderas av misstag om de utsätts för ett yttre magnetfällt. Nackdelen med kort med hög koercivitet är att dessa kräver speciell utrustning för att skrivas. De kort som används som bankkort har oftast en låg koercivitet. Magnetremsan på ett bankkort delas upp i tre spår, mängden data på varje spår och användningen av dem regleras i ISO-standarder. [1]

De standarder som gäller för magnetkort är ISO 7810, 7811 och 7813. Det två första standarderna beskriver tillsammans alla egenskaper hos magnetkorten så som de fysiska egenskaperna (storlek, tjocklek, värmetålighet, material mm), utformningen av magnetremsan, spårplaceringen på denna, koerciviteten samt hur och var tecknen på kortet ska präglas in. Den sista, 7813, beskriver enbart kort för finansiella transaktioner (t.ex. bankkort) och behandlar bland annat mängden data på varje spår. [1]

6. Chipkort

Den nya typen tekniken som används på bankkort är chipkort. De chip som används innehåller mikroprocessor, serieport och minnen. Vanligtvis är det en 8-bitars mikroprocessor, en seriell port och tre

This watermark does not appear in the registered version - http://www.clicktoconvert.com

minnen. Det första minnet är ett ROM som innehåller själva programmen och annan statisk data som är gemensam för alla kort. Det andra minnet är ett EEPROM som innehåller information specifik för varje kort så som namn och konto-nummer till den registrerade ägaren och krypteringsnycklar. Dessa två minnen är enbart läsbara medan det tredje minnet som är ett RAM-minne både är läs- och skrivbart och används under exekveringen. För kommunikation med kortet finns en seriellport för in och utdata. Det finns också kontakter för ström, klocka och för att starta om kortet. Om kortet ska klara av kryptering med asymmetriska metoder utrustas de ofta med en hjälpprocessor som utför beräkningarna med stora heltal och exponenter. [2]

Genom att använda chipkort istället för magnetkort uppnås en högre säkerhet då chipkort är betydligt svårare att kopiera all information från än magnetkort. I chipkort finns det också möjlighet att gömma vital information på så sätt att informationen inte kan läsas utifrån utan enbart är tillgänglig internt på chipet och alltså inte kan kopieras alls. På magnetkort används idag ett system med vattenmärkning som inte kan kopieras från korten, detta system är dock långt ifrån perfekt och fungerar enbart i uttagsautomater. Ytterligare en funktion som finns på chipkorten och som kan användas för att öka säkerheten är att de själva kan kryptera den information som de gör tillgänglig för yttervärlden. Ytterligare en fördel med chipkorten är att de inte riskerar att raderas av misstag så som magnetkorten med låg koercivitet gör. [4, 5]

För chipkort finns ISO-standarden 7816 som bland annat behandlar chipens utformning, elektroniska signaler samt kommunikationsprotokoll. [1]

7. Säkerhet i de nya bankkorten

I detta avsnitt kommer vi att behandla säkerheten som implementerats i de nya chipkorten. Materialet är hämtat från [4] men också till viss del från [5].

7.1. EMV-standarden

1999 skapade Visa International och MasterCard International tillsammans EMVco, en organisation som har satt upp en standard för chip: EMV-standarden. [3] Denna standard bygger på ISO 7816 och tar upp mycket av de säkerhetsfrågor som ligger till grund för de nya, säkrare, bankkorten. EMV är den standard som både Föreningssparbanken och Nordea använder i sina chip. Deras chip kallas därför EMV-chip.

7.2. EMV-chip

Chipen som används i de nya bankkorten tillverkas av globala chiptillverkare som producerar själva chipet efter EMV-standarden. Vissa maskin-instruktioner ingår då. Därefter går chipen vidare till företag som lägger på operativsystem och applikationer (ofta svåra att skilja på). Som sista steg i produktionskedjan går chipen till en så kallad service provider (XPonCard) som gör chipen personliga genom att lägga in enskilda kunders personliga information.

Nordea och Föreningssparbanken använder båda XPonCard som service provider. Nordea lägger in beställningar på chip och överför datafiler med sekretessbelagd data krypterad med trippel-DES och signerad med en hashfunktion. XPonCard tar alltså aldrig del av denna information. [4]

Nordea och Föreningssparbanken har valt att implementera chip av olika säkerhetsgrader. Föreningssparbanken använder sig av ett SDA-chip (Static Data Authentication) medan Nordea använder ett mera avancerat DDA-chip (Dynamic Data Authentication) som innehåller en extra mikroprocessor. Anledningen till att Nordea valt det mer avancerade chipet är att de önskar kunna lägga in mer funktionalitet i chipet i framtiden.

Vid skrivning av data på EMV-chipet sätts olika attribut på datan för att ge läs och skrivrättigheter. Data som vid införandet klassas som lässkyddad går inte att komma åt från externa källor efter skrivningen och är därmed säkrad från kopiering. Detta leder till att trots att vissa delar av chipet är kopieringsbara så fungerar inte en kopia av chipet i en EMV-betalterminal. Attributen medför alltså ett kopieringsskydd men också att man på ett säkert sätt kan lagra konfidentiell data på chipet, till exempel nycklar och PIN-koder.

7.3. EMV-terminaler

EMV-standarden specificerar förutom chipspecifik säkerhet också den säkerhet som måste förekomma i EMV-terminaler, särskilt i kommunikationen mellan tangentenheten som används av kunden för att slå in PIN-koden och kortläsaren där kunden sätter in sitt chipkort.

Nordea använder en lösning som kallas PKI och som bygger på RSA och därmed asymmetriska nycklar. Vid insättning av ett kort i kortläsaren skickar kortet en publik nyckel till tangentenheten. Tangentenheten använder sedan denna nyckel för att kryptera PIN-koden som kunden slår in innan den skickar den krypterade koden till chipkortet. Chipkortet avkrypterar PIN-koden med en privat (hemlig) nyckel och jämför den med en PIN-kod som finns lagrat i chipet. Både den privata nyckeln

This watermark does not appear in the registered version - http://www.clicktoconvert.com

och PIN-koden ligger lagrade på chipet med attributet satt för att förbjuda läsning och är på det sättet skyddade mot kopiering.

PKI är den funktion som i framtiden ska möjliggöra kortens användning som elektroniskt ID.

8. Varför chipkort?

Det huvudsakliga syftet med uppgraderingen av bankkorten från magnetkort till chipkort är att göra korten svårare (förhoppningsvis omöjliga) att kopiera och därmed öka säkerheten. Nordea har dessutom passat på att lägga till andra funktioner i chipet för att det i framtiden ska kunna användas bl.a. som identifierare vid inloggning på Internet.

Orsaken till att en satsning gjort på denna teknik just nu är det ökade intresset i Europa för att minska problemet med s.k. skimming, kopiering och förfalskning av magnetkort. De svenska bankerna har varit oroliga för att en trend ska uppstå där internationella ligor söker sig till Sverige om inte samma säkerhetsnivå hålls. [5]

9. Information i tidningar och tidskrifter

Vi kommer här att redovisa för den information vi hittat angående säkerheten i de nya bankkorten i svenska dagstidningar och i tidsskrifter med datateknisk inriktning.

9.1. Informationssamlande

Varken dagstidningar eller tidskrifter har någon omfattande information om chipkorten och bytet från magnetkort till chipkort. Vid sökningar i mediearkivet med flera olika kombinationer av sökord hitta vi endast ett fåtal artiklar från det senaste året. Det tidningar som information hittades i var främst Computer Sweden och lokala dagstidningar som tagit sitt material från TT. När det gäller tidskrifter har vi begränsat oss till svenska sådana men där har vi inte hittat några artiklar alls inom ämnet.

9.2. Information från artiklar

Den information som finns i artiklarna går främst ut på att de nya korten med chip är säkrare än de gamla med magnetremsa. Det främsta säkerhetshotet mot korten anges vara kortbedrägerier där personers kort kopieras utan deras vetskap och sedan används vid köp (skimming). Detta är enligt källorna lätt att genomföra med magnetkortstekniken medan de nya korten med datachip ska vara betydligt svårare att kopiera. [6, 7, 10] I artiklarna påpekas det även att korten till att börja med kommer att ha både magnetremsa och chip och att magnetremsan på korten fortfarande kommer att vara lika lätta att kopiera. [8, 10]

En annan fördel som ofta tas upp i artiklarna är att chipkorten ger möjligheter till att inkludera flera funktioner, vanliga exempel är elektroniskt ID, möjlighet att ladda ner biljetter till kortet och anpassade bonussystem. [8, 9, 10]

Det som är den främsta anledningen till att svenska banker väljer att byta ut sina kort nu är att de från och med 2005 själva kommer att vara tvungna att betala för de kortbedrägerier som sker med kort utan chip. Detta är något idag betalas av kreditkortsbolagen. [8, 10]

Chipkorten anges följa en internationell standard framtagen av Visa och Mastercard och har redan införts i flera länder i Europa. [8, 10] Bytet till nya kort beräknas ta 2 år för Nordea och det är tänkt att kunderna inte ska märka någon skillnad när det gäller den vanliga användningen av korten. [10]

Informationen i artiklarna är troligen lättförståeliga även för personer utan it-bakgrund. De artiklar vi har funnit har inte riktat sig mot mer säkerhetskunniga personer. Djupare information saknas helt.

10. Information från bankerna

Här följer redovisningen av information vi fått angående säkerheten i chipkorten ifrån de berörda bankerna. Den största delen av informationen är hämtad från telefonsamtal till och personliga intervjuer med bankpersonal.

10.1. Utskick till kund

Nordea har en folder som de skickar ut till sina kunder tillsammans med de nya chipkorten. Där uppges syftet med bytet vara att ”För att höja säkerheten och minska risken för bedrägerier med förfalskade kort […]” Kortet är enligt foldern omöjligt att kopiera. Det ”använder avancerad teknik för att skydda informationen och garantera att kortet är äkta.” För vidare information om chipkorten hänvisar foldern till en central kortservice som kan nås på telefon på vanliga kontorstider. [11]

Föreningssparbanken har ännu inte lanserat sina kort, men lanseringen ligger i en nära framtid och deras utskick kommer också att innehålla en folder som redan nu är framställd. Den foldern kommer dock inte att innehålla någon information om chipkorten i sig. Den enda sådana beskrivning som går att finna är i bruksanvisningen för internationella bankkort där det finns en kort introduktion till de nya chipkorten men inget alls om säkerheten i dem. [12]

Nordeas folder innehåller enligt oss troligen all den information som en ”vanlig” kund kan tänkas ha

This watermark does not appear in the registered version - http://www.clicktoconvert.com

behov av. Informationen är också lätt att ta in av personer utan it-bakgrund.

10.2. Hemsida

Varken på Nordeas eller på Föreningssparbankens hemsida finns någon information om de nya chipkorten. Från Nordeas sida finns dock länkat vidare till Visas europeiska sida där det finns en del grundläggande information om chipkorten. Där kan man läsa att anledningen till bytet av kortteknik är att korten blir säkrare och robustare, transaktionerna går snabbare och att det finns möjligheter att ge korten nya funktioner. Informationen på denna sida är på engelska.

Hemsidorna innehåller alltså ingen information alls angående säkerheten i och runt chipkorten.

10.3. Lokala bankkontor

På Nordeas och Föreningsparbankens lokala kontor i Linköping kan personalen få information om de nya chipkorten via intranätet. På Nordea där införandet av chipkorten redan är på gång har personalen också fått internpost om dem. De anställda som är mer direkt berörda har dessutom fortgående fått mer information på gruppmöten. Huvudansvaret för informationsutdelning till kunder på Nordea ligger på huvudkontoret i Stockholm och kortservicen där. Lokalkontoren har i allmänhet inte någon detaljerad information utan har en personalservice i anknytning till huvudkontoret dit de anställda kan ringa och få svar på frågor. Personalen på banken är också duktiga på att hänvisa till mera insatta personer vid frågor de saknar kunskap att besvara. På båda bankernas lokala bankkontor är det meningen att personalen ska kunna svara på de frågor den genomsnittlige kunden kan tänkas ha. De flesta kunder borde inte ha något intresse av specifika frågor angående säkerhet och teknik. [13, 14]

En it-intresserad person kan knappast räkna med att få de svar de är intresserade av på ett lokalt bankkontor.

10.4. Kortservice

Nordea hänvisar som ovan nämnts till en kortservice i den folder de skickar ut med de nya korten. Den information man kan få om säkerheten i korten på denna tjänst är att kortet inte går att kopiera på samma sätt som de tidigare magnetkorten. Vid närmare utfrågning uppgavs anledningen till detta vara att det inte går att avläsa informationen som finns på chipet. Varje chip är unikt och det innehåller ”en egen hårddisk som en dator” som gör att det inte går att kopiera den exakt rätta informationen. Genom detta kan kortläsarna som korten används i se om kort är äkta. [15]

Vi anser inte att informationen som kortservicen gav skulle räcka för att besvara de frågor som en it-intresserad kan tänkas ha. Den duger dock säkert bra till att besvara den genomsnittlige kundens frågor.

10.5. Teknisk information

Som säkerhetsspecialist kan man (efter diverse omdirigeringar) få prata med en av de ansvariga för de nya chipen på Nordea. Där kan även säkerhetskunniga få bra, detaljerade svar på tekniska frågor om den säkerhet som Nordea står för i korten. Föreningssparbanken hänvisar teknikfrågor till den konsult som är ansvarig för deras projekt.

11. Avslutning

Säkerheten i de svenska bankernas nya chipkort ligger mycket i chipet i sig. Nordea och Föreningssparbanken har stor tillit till säkerheten som specificeras i EMV-standarden och därmed finns inbyggd i EMV-korten. Den säkerhet som bankerna själva implementerar handlar till största del om de metoder de väljer för att kryptera och signera transaktioner av data. Även för dessa finns det specifikationer i EMV-standarden. [4]

Säkerheten i chipkorten kommer att vara högre än i de nuvarande magnetkorten när teknikbytet är helt genomfört, risken för bedrägeri med förfalskade kort kommer att vara mindre [11]. Nordeas bankkort är under övergångstiden utrustade med både ett fungerade chip och en fungerande magnetremsa vilket gör att korten fortfarande är känsliga för s.k. skimming. Båda typerna av kort är förstås lika känsliga för stöld och dylika problem.

Vi är förvånade över den brist på information om chipkorten som finns i tidningar och tidskrifter. Den information som vi funnit i dagstidningarna riktar sig helt mot den genomsnittliga svensken, och tar upp ämnet mycket översiktligt och utan någon som helst förklaring till tekniken. Men det är långt ifrån alla tidningar som tagit upp ämnet över huvudtaget. Det faktum att det skrivs så lite om ämnet tyder på att intresset ute hos allmänheten för att läsa om det är litet. Det som däremot är underligt är att det inte finns någon information alls för en person med ett större intresse och kunnande, finns inte sådana personer? Ämnet har inte tagits upp i någon teknisk tidskrift som vi kunnat finna och de artiklar som funnits i Computer Sweden har legat på en översiktlig nivå och fokuserat på de möjliga extrafunktionerna hos chipkorten. Det går överhuvudtaget inte att finna någon information om varför chipkorten blir säkrare än magnetkorten i någon tidning.

This watermark does not appear in the registered version - http://www.clicktoconvert.com

Vi anser att både Nordea och Föreningssparbanken är dåliga på att informera sina kunder om detaljerna angående säkerheten i den nya chiptekniken. Nordeas folder som finns med i utskicket av de nya bankkorten informerar i korta ordalag om den ökade säkerheten, men varken på bankkontor eller på kortservicen kan man få förklaring på hur denna säkerhet uppnås. Föreningssparbanken kommer inte ens att skicka med en folder med information om korten tillsammans med sina nya chipkort när dessa lanseras [12].

Denna brist på information behöver inte vara av ondo då den genomsnittlige kunden oftast inte är intresserad av detaljerna. För dem är troligen intresset större för säkerheten i kortnummer, oftast i samband med internetbetalningar. Att ingen information alls finns på de berörda bankernas hemsidor anser vi vara en miss.

Som it-intresserad eller säkerhetsexpert får man enligt vår erfarenhet uppsöka samma källa: personer inblandade i chipkortprojektet, troligen på bankens it-avdelning. Försöker man komma fram till dessa via bankernas centrala telefonväxel kan man få passera många mellanpersoner, t.ex. personer från kortavdelningen och säkerhetsavdelningen, vilka inte har några detaljerade svar att ge men gärna skickar en vidare. Väl i kontakt med en insatt person kan man få svar på de flesta frågor man kan tänkas ha, in i detalj om intresse finns men risken är nog stor att många intresserade skulle ge upp på vägen.

Allt som allt uppfattade vi bankerna som mycket tillmötesgående och villiga att hjälpa till så långt de kunde. Personkontakt krävdes dock och ett stort antal telefonsamtal för att få tag på rätt person att prata med.

På våra lokala bankkontor här i Linköping visste personalen inte alls mycket om chipkorttekniken. Den information de kunde ta fram var på båda bankkontoren ungefär den information som fanns i Nordeas folder: att säkerheten ökats och att kortet gjorts kopieringsskyddat. Vi anser inte att det är något problem att personalen på dessa kontor saknar djupare kunskaper då de säkerligen inte får många frågor i ämnet och om de får det verkar mycket villiga att hjälpa en att ta reda på var informationen finns att hämta.

12. Referenser

[1] H. Hallbäck, and M. Mischel, *Teoretiska och praktiska attacker mot magnetkort och smarta kort* , Projekt i kursen TDDC03, Linköping, 2003

[2] R. Andersson, *Security Engineering* , Wiley, New York, 2001

[3] www.emvco.com, 2004-04-22

[4]Telefonintervju: Jonas Wihager; Nordeas itavdelning Stockholm, 25 min , 2004-04-23

[5] Telefonintervju: Ulf Almqvist; Konsult för Föreningssparbanken på cipkortprojektet, 15 min, 2004-04-27

[6] B. Ljungdahl, "Microchip ska förhindra kortbedrägerier", *Helsingborgs dagb lad*, 2004-03-10, s.9 och *Hallands Nyheter* , 2004-03-10, s.13

[7] A. Wennerstrand, "Bakkkort korieras med enkel apparat", *Helsingborgs dagblad* , 2003-07-30, s.8

[8] L. Aspelin, "Dags för säkra kort", *Svenska dagbladet* , 2004-01-17, s.48

[9] K. Lindström, "Nordeas bankkort förses med e-id", *Computer Sweden* , 2003-06-02, s.6

[10] T. Bjurman, "Bankerna byter ut alla kort", *Computer Sweden* , 2004-01-16, s.5

[11] Nordea folder: *Ditt kort med nytt chip*

[12] Telefonintervju: Gunhild Swan; Föreningssparbankens itavdelning Stockholm, 15min, 2004-04-22

[13] Intervju: Dennis och Sofia; Nordeas lokalkontor Linköping, 25 min, 2004-04-26

[14] Telefonintervju: Rune Karlsson; Föreningssparbankens lokalkontor Linköping, 15 min, 2004-04-27

[15] Telefonintervju: Nordeas kortservice, 10min, 2004-04-27