PATENTBESVÄRSRÄTTENS

DOM

meddelad 2008-01-31 efter överklagande av Patent- och registreringsverkets beslut, se bilaga 1.

Klagande: 1. Försvarets materielverk (invändare 1)
2. Telefonaktiebolaget L M Ericsson (invändare 2)

Ombud för 1: Dag Hedefält
Ombud för 2: Dr Ludvig Brann Patentbyrå AB

Motpart: IMP International AB (patenthavare)

Ombud: Awapatent AB

Målet gäller: Upphävande av patent på metod och system för kryptering och autentisiering.

DOMSLUT

Patentbesvärsrätten undanröjer överklagade beslutet och upphäver patentet.

Postadress	Besöksadress	Telefon	Fax	Org.nr
Box 24160 104 51 Stockholm	Linnégatan 87 D	08-783 38 50	08-783 76 37	202100-3971

REDOGÖRELSE FÖR SAKEN OCH FRAMSTÄLLDA YRKANDEN

IMP International AB ansökte den 24 mars 2000 om patent på en uppfinning benämnd ”Metod och system för kryptering och autentisiering”. Patent meddelades den 11 juni 2002.

I den till ifrågavarande patent hörande beskrivningen anges följande om uppfinningens bakgrund och syfte.

> Föreliggande uppfinning hänför sig till en metod och ett system för en säker krypterad överföring eller autentisiering mellan åtminstone två enheter via en osäker kommunikationskanal.
>
> Det är normalt svårt att erhålla en säker krypterad överföring mellan enheter över osäkra kommunikationskanaler, såsom över allmänna telefonlinjer, datanätverk, vid radioöverföring osv. Konventionella krypteringsalgoritmer kräver att nycklar överförs mellan enheterna, i form av privata eller allmänna nycklar. Denna överföring av nycklarna innebär dock praktiska problem. Nycklarna kan överföras på separata, säkra kanaler, men detta är besvärligt, dyrt och tidsödande. Alternativt kan nycklarna överföras via den osäkra kanal över vilken den krypterade överföringen sedan skall ske. Detta innebär dock en betydande säkerhetsrisk. Även då krypton med s k öppen nyckel används, såsom RSA-systemet, innebär överförandet av nyckeln att större och mer komplicerade nycklar och krypteringsalgoritmer krävs för att den krypterade överföringen skall vara tillräckligt säker, och detta innebär naturligtvis ökade besvär och kostnader. Likartade problem gäller för att med konventionella metoder erhålla en säker verifiering av enheter, s k autentisiering, över osäkra kommunikationskanaler. Sådan autentisiering bygger på att data överförs mellan enheterna, där denna data bygger på en unik nyckel. Exempelvis kan nyckeln användas för att kryptera en kontrollsumma som bygger på ett sänt eller mottaget meddelande. Samma problem som för annan krypterad överföring vad gäller överföringen av nycklar mellan enheterna gäller dock även i detta fall.
>
> Det är därför ett syfte med föreliggande uppfinning att tillhandahålla en metod och ett system för krypterad överföring och autentisiering över en osäker kommunikationskanal som helt eller åtminstone delvis löser de ovan relaterade problemen hos den kända tekniken.

Försvarets materielverk (FMV) och Telefonaktiebolaget L M Ericsson (Ericsson) gjorde invändning mot det meddelade patentet.

FMV anförde till stöd för sin invändning att uppfinningen saknade nyhet eller i vart fall uppfinningshöjd i förhållande till dels två olika dokument, D1 och D2, dels ”notoriskt kända förfaranden vid substitutionschiffer, blankettchiffer, nyckelordschiffer och användning av

försvarets täcktabeller".

D1 "Applied Cryptography", av B. Schneier, John Wiley & Sons Inc., 1994
D2 "Cipher Systems, The Protection of Communications" av H. Beker och F. Piper, Northwood Publications, 1982

Ericsson anförde till stöd för sin invändning att uppfinningen saknade nyhet eller i vart fall uppfinningshöjd i förhållande till två andra dokument, D3 och D4.

D3 "Specification of the Bluetooth System" Version 1.0 B, s. 1-4, 48,49, 87, 123, 126, 149-178, publicerad 1 december 1999
D4 TS 100 929 V6.0.1 (1998-07) "Digital cellular telecommunications system (Phase 2+); Security related network functions (GSM 03.20 version 6.0.1, Release 1997), s. 1-2 och 48-51

Patentverket, som i överklagade beslutet fann att uppfinningen enligt de beviljade patentkraven var ny och skiljde sig väsentligen från den anförda kända tekniken, avslog invändningarna.

Yrkanden m.m.

Invändarna har i Patentbesvärsrätten vidhållit sina yrkanden att patentet skall upphävas.

Patenthavaren har i första hand bestritt ändring. I andra hand har patenthavaren yrkat att patentet upprätthålls med patentkrav som inkom den 21 juni 2004. I sista hand har patenthavaren yrkat att patentet upprätthålls med patentkrav märkta tredjehandsyrkande respektive fjärdehandsyrkande, inkomna den 28 maj 2007.

Uppfinningen definieras i de beviljade och i första hand åberopade självständiga patentkraven 1 och 8 enligt följande.

l. Metod för krypterad överföring eller autentisiering mellan åtminstone två enheter i ett datakommunikationssystem via en osäker kommunikationskanal, omfattande stegen att:
- vid en initieringsprocedur komma fram till ett gemensamt utgångsvärde för användning i respektive enhet;
- synkroniserat och periodiskt uppräkna ett räknevärde hos vardera enheten;
- vid vardera enheten, oberoende av varandra, generera en nyckel utifrån utgångsvärdet samt räknevärdet; och

- använda dessa sålunda genererade nycklar vid en efterföljande krypterad överföring eller autentisiering.

8. Datakommunikationssystem för krypterad överföring/autentisiering mellan åtminstone två enheter via en osäker kommunikationskanal, varvid vardera enheten omfattar en nyckelgenereringsenhet, vilka nyckelgenereringsenheter omfattar ett minne i vilket identiska utgångsvärden lagrats, en räknare för periodisk och mellan enheterna synkroniserad förändring av ett räknevärde, samt en beräkningsenhet vilken är inrättad att i vardera enheten, oberoende av andra enheter, automatiskt generera en nyckel utifrån utgångsvärdet samt ett räknevärde från räknaren, vilka nycklar kan användas för krypterad överföring eller autentisiering mellan enheterna.

De i andra hand åberopade självständiga patentkraven 1 och 7 har följande lydelse.

1. Metod för krypterad överföring eller autentisiering mellan åtminstone två enheter i ett datakommunikationssystem via en osäker kommunikationskanal, omfattande stegen att:
- vid en initieringsprocedur komma fram till ett gemensamt utgångsvärde för användning i respektive enhet;
- synkroniserat och periodiskt uppräkna ett räknevärde hos vardera enheten;
- vid vardera enheten, oberoende av varandra, generera en nyckel utifrån utgångsvärdet samt räknevärdet; och
- använda dessa sålunda genererade nycklar vid en efterföljande krypterad överföring eller autentisiering; varvid enheterna efter en inledande synkronisering av räknarna endast utför kompletterande synkroniseringssteg vid behov.

7. Datakommunikationssystem för krypterad överföring/autentisiering mellan åtminstone två enheter via en osäker kommunikationskanal, varvid vardera enheten omfattar en nyckelgenereringsenhet, vilka nyckelgenereringsenheter omfattar ett minne i vilket identiska utgångsvärden lagrats, en räknare för periodisk och mellan enheterna synkroniserad förändring av ett räknevärde, samt en beräkningsenhet vilken är inrättad att i vardera enheten, oberoende av andra enheter, automatiskt generera en nyckel utifrån utgångsvärdet samt ett räknevärde från räknaren, vilka nycklar kan användas för krypterad överföring eller autentisiering mellan enheterna, varvid enheterna är inrättade att avkänna när de inte är synkroniserade och endast därvid vidtaga åtgärder för att återställa synkroniseringen.

Följande yrkanden motsvarar första- resp. andrahandsyrkandet i angiven ordning med den skillnaden att de anger ”kryptering och autentisiering” i stället för ”kryptering eller autentisiering” resp. ”kryptering/autentisiering”.

Grunder m.m.

Var och en av invändarna har som grund för sitt yrkande hållit fast

vid att den i patentkraven angivna uppfinningen saknar nyhet och uppfinningshöjd. Vidare har Ericsson i Patentbesvärsrätten som en ny grund åberopat att beskrivningen av uppfinningen inte är så tydlig att en fackman med ledning av den kan utöva uppfinningen.

FMV har i Patentbesvärsrätten åberopat ytterligare tre dokument, D5, D6 och D9 samt ytterligare avsnitt ur D2 (sidorna 285-287, benämnt D2´). FMV har här frånfallit hänvisningen till försvarets täcktabeller. Eriksson har åberopat två nya dokument, D7 och D8.

D5 Amerikanska patentskriften US 4 720 860
D6 ”Wesen und Bedeutung kryptographischer Schlüssel”, doktors-avhandling vid universitetet i Linz, 1996, av Otto J Horak
D7 RFC 2246, ”The TLS Proocol”, version 1.0
D8 WO 95/15629, A1 (senare frånfallen)
D9 ”Handbook of applied Cryptography”, av Alfred J. Menezes m fl., CRC Press 1996

Som grund för sina yrkanden har patenthavaren hållit fast vid att uppfinningen definierad i patentkraven uppvisar nyhet och uppfinningshöjd. Vidare har patenthavaren anfört att patentet i sin helhet beskriver uppfinningen på ett så tydligt sätt att den kan utövas av en fackman inom området.

Utveckling av talan

FMV har till utveckling av sin talan anfört i huvudsak följande.

”Notoriskt kända förfaranden”

Uppfinningen tar upp en mycket gammal krypteringsteknik och flyttar över den till datakommunikationsområdet. Vi hävdar att denna överflyttning inte kan motivera ett patentskydd. Nu påstår PRV i avslagsbeslutet att de gamla krypteringstekniker vi anfört inte utför detsamma som vid uppfinningen. Härvid presenterar PRV ett par påståenden som är helt felaktiga. Sålunda står det i avslagsbeslutet beträffande blankettchiffer att "den ene användaren ... överför... först ett nyckelnummer med vilket den påföljande texten är krypterad, sedan skickas själva informationen".

PRV:s påstående om att man i blankettchiffer måste sända blankettnumret först är inte sant. Blanketterna används ofta i tur och ordning, vilket möjliggör att man inte behöver sända något inledande blankettnummer. - Den risk man tar är naturligtvis att något meddelande kan komma bort varvid man kommer ur synkronisering. Det är emellertid precis samma risk som man löper med förfarandet

vid patentet; skickar man ingen synkroniseringsinformation är man beroende av att alla meddelanden kommer fram. - - - Det är alltså för att undanröja risken med att tappa ett meddelande som man ofta, men alls inte alltid, överför nyckelnumret först. Detta innebär dessutom ingen säkerhetsmässig försvagning eftersom det inte är en "arbetande nyckel" man överför utan ett räknevärde som lokalt och parallellt kombineras med en "basnyckel" (= utgångsvärde) för att få den "arbetande nyckeln". När det gäller andra typer av "notoriskt kända förfaranden" är det helt felaktigt påstå att ett nyckelnummer först måste överföras vid en transmission. Vid exempelvis användning av täcktabell i militär foni sker inte detta. Här används under en förutbestämd, och för alla inblandade känd, tid en viss täckordstabell. Alla meddelanden under den aktuella tiden krypteras med samma tabell, utan någon överföring av räkneord eller dylikt. Nästa period används nästa täckordstabell o.s.v. Detta är ett allmänt känt - notoriskt känt - förfarande. ---

PRV hävdar vidare att inga nycklar genereras vid dessa "notoriskt kända förfaranden", utan att man använder på förhand genererade nycklar. Vi har beträffande detta redan framfört i invändningsskriften att en uppsättning blanketter, nyckelord eller annan gemensam hemlighet måste betraktas som det "gemensamma utgångsvärdet" i patentet. Kombinationen med ett "räknevärde" - ofta ett löpnummer (blankettnummer), ett datum eller ett klockslag - ger sedan (=genererar) den slutliga kryptonyckeln (=den arbetande nyckeln) som används för ett visst meddelande. ---

Vi hävdar med eftertryck att en uppsättning blanketter, nyckelord eller annan gemensam hemlighet är ett utgångsvärde och att en kombination med ett räknevärde som ger en delmängd av detta utgångsvärde innebär en generering av en arbetande nyckel enligt patentet. - - -

Vi hävdar att det idag måste vara omöjligt att patentera ett förfarande som, utom sitt medium (=datakanalen), helt överensstämmer med känd kunskap. Speciellt stöd för vår åsikt att det är närliggande att göra en koppling mellan gamla förfaranden, äldre än datamaskinen, och krypteringsförfarande för datakommunikation har vi i D2, s. 295-296, där denna koppling görs mellan blankettchiffer och en form av modern kryptering i datakommunikationssammanhang.

D1

I kapitel 7 behandlas nycklar och deras generering. På sidan 145 anges hur man genererar nycklar enligt ANSI X9.17-standarden. De nycklar man talar om här är de nycklar som i den grundläggande krypteringsfiguren skall användas för att kryptera klartext, dvs. den arbetande nyckeln. Nycklarna används för att kryptera enligt någon känd metod, DES nämns som en bland flera. – Härvid motsvarar k patentets "utgångsvärde" och benämns i beskrivningar av kryptoteknik ofta "basnyckel" eller "gemensam hemlighet". V_0 är ett startvärde, T är ett räknevärde och resultatet R_i är den resulterande kryptonyckeln - den arbetande nyckeln. Det visas här hur den arbetande nyckeln R_i genereras utifrån "utgångsvärdet" k och "räknevärdet" T. Det är således från D1 helt känt att utföra de steg som anges i patentkravet 1 i patentet. - - -

PRV framhåller i avslagsbeslutet att D1 inget säger om att [den arbetande] nyckeln genereras synkroniserat och oberoende i minst två enheter. Det är riktigt att detta inte står explicit. Samtidigt är detta för en fackman på området fullständigt självklart att man gör så. Ingen transmitterar någonsin en genererad "arbetande nyckel" över en osäker kanal. Det är så självklart att det inte behöver sägas i en bok för fackmän. - PRV anför vidare att det i stället i D1 anges att

nycklar överförs och menar uppenbarligen "arbetande nyckel". Detta är en uppenbar övertolkning. För fackmannen är det självklart att det som skall överföras, och då på ett säkert sätt, är det som med det aktuella patentets terminologi kallas "utgångsvärden" - en genererad "arbetande nyckel" överför man självklart inte på en osäker kanal. - Rent generellt används ordet "nyckel" slarvigt i flera betydelser, vilket visas inte minst i detta ärende. Det faktum att ordet "nyckel" används i flera betydelser gör att all text måste läsas med fackmannens förståelse för innehållet, så att inte allt som någonstans av någon kallas "nyckel" schablonmassigt anses vara detsamma.

Vi hävdar således att det är självklart vid tillämpning av X9.17-standarden att utföra beräkningarna hos vardera kommunikationsparten. Också i jämförelse med detta förfarande måste patentets förfarande anses närliggande och därmed inte patenterbart.

D2

Kapitel 8.2, "Key structure" berör hur nycklar skapas och används. I figur 8.1 visas grunden för s.k. strömkryptering (stream cipher). En grundläggande kryptering i enlighet med vad som anförts ovan motsvaras här av burken "Algorithm" och summeringen. ---I figur 8.2 visas hur nyckeln till burken "Algoritm" - den arbetande nyckeln - skapas i vad som här kallas "Mixer" i beroende av "Base key", vilket motsvarar "gemensamt utgångsvärde" i patentets krav 1 och "message key", vilket, som vi i nästa stycke kommer att visa, kan motsvara "räknevärde" i patentkravet 1. Det är därigenom från D2 helt känt att utföra de steg som anges i patentkravet 1 i patentet.

När det gäller "message key" anges på sidan 299 i D2 hur man, efter ett inledande initialskede, kan arbeta utan en yttre "message key". I stycket beskrivs hur man lokalt och distribuerat kan beräkna en aktuell arbetande nyckel utgående från ett känt "utgångsvärde" och ett på känt sätt framräknat "räknevärde". Detta kallas i boken för "flywheeling". ---

Patentkravet 1 anger "en metod för krypterad överföring eller autentisiering" och patentkravet 8 anger ett "datakommunikationssystem för krypterad överföring/autentisering". Patentkravet 8 följer till sitt tekniska innehåll fullständigt patentkravet 1. Det är endast fråga om ett sådant byte mellan olika kategorier, såsom en metod och en anordning, som inte i sig medför någon patenterbarhet. Patentkravet 8 är därför inte patenterbart på samma grund som patentkravet 1 inte är det. ---

När det sedan gäller vad vi framfört om kryptering av moderna datakommunikationssystem i D2, noterar vi att PRV i avslagsbeslutet, sidan 3 första stycket, instämmer i vad vi anfört om att såväl ett förfarande med överföring av en synkroniseringsinformation (message key), som utan sådan synkroniseringsinformation (flywheeling) är känd och använd i D2 och känd och använd i det aktuella patentet.

Skillnaden mellan de två förfarandena har vi /…/ utvecklat genom att påpeka att det som är ett undantag i det ena fallet är regel i det andra och vice versa. Det är fråga om en glidande skala mellan ytterligheter och det är självklart att en uppfinning inte blir patenterbar bara för att man förskjuter fokus. I det ena fallet är ambitionen att sända synkroniseringsinformation, men ibland tappar man den och får arbeta utan synkroniseringsinformation. I andra fallet är ambitionen att inte överföra synkroniseringsinformation, men ibland måste man överföra sådan information. --- PRV har i motsats till oss ansett att om två förfaranden är kända,

det ena back-up för det andra, så är det patenterbart att använda back-up-förfarandet som huvudalternativ med det andra kända förstahandsvalet som reserv. Vi delar som sagt inte denna uppfattning och hävdar med visst eftertryck motsatsen. Uppfinningen är därför inte patenterbar med hänsyn till D2.

I **D2'** visas också andra förfaranden där en "message key" inte sänds först. Det är således inte bara vid flywheeling enligt s. 299 som detta sker. I kapitlet 7.4, sidan 285-287 /…/ visas i figur 7.10 hur ett blockkrypto fungerar. Klartext i block, därav ordet blockkrypto, kommer från vänster och kombineras med en arbetsnyckel uppifrån, vilket leder till kryptotexten till höger.

I grundformen enligt figuren krypteras all klartext med samma arbetande nyckel. Detta är inte lämpligt under någon längre tid; kanske inte ens för två datablock. Alltså måste den arbetande nyckeln modifieras mellan olika meddelanden och i figur 7.11 visas hur en basnyckel till vänster modifieras genom ett feedbackförfarande överst så att det i "block cipher algorithm" skapas en arbetande nyckel från basnyckeln och det värde som räknas fram i feedback-loopen. Den arbetande nyckeln sparas i register B och kombineras sedan med klartexten, här kallad data, till kryptotexten. Omvändningen sker på mottagarsidan. Förfarandet kallas ibland "counter mode" och finns också beskrivet i D1, s. 163. - Också i jämförelse med detta förfarande som separat och parallellt kombinerar en basnyckel med ett räknevärde, jfr benämningen "counter mode", måste patentets förfarande anses känt eller närliggande och därmed inte patenterbart.

D5

Denna skrift visar ett förfarande som helt föregriper det nu aktuella patentet. - För att beskriva vad detta patent visar använder vi det referat samme sökande gör av detta sitt patent i sitt senare amerikanska patent 5,168,520. I detta står: "U.S. Pat. No. 4,720,860, discloses a personal identification system wherein the individual has a card or other small, portable device which contains a microprocessor programmed to utilize a secret algorithm to generate a nonpredictable number from a stored value unique to the individual and a time varying value provided for example by a clock. The nonpredictable value is preferably displayed on the device. The individual then enters his secret PIN into a central verification system, either directly or over a telephone line, causing the central system to access stored information corresponding to the individual and to utilize at least some of this information to generate a nonpredictable value at the central computer utilizing the same algorithm as at the individual's microprocessor. At the same time this is being done, the individual is entering the number appearing at that period of time on the display of his device. The two values will match, signifying identification of the individual, only if the individual has entered the correct PIN and if the individual has the proper device so that the nonpredictable code displayed corresponds to that being generated at the central verification computer.

Att det är fråga om en samtidig, oberoende generering av kod hos två parter som skall kommunicera med varandra framgår dessutom tydligt bl.a. i patentkravet 1 där det står: "said first and second computer means independently generating said first and second non-predictable codes for comparison thereof...".

Det är omedelbart klart från detta att patentet visar

- en metod för autenticering mellan två enheter i ett datakommunikationssystem via en osäker kommunikationskanal

och att man utför stegen

- att vid en initieringsprocedur komma fram till ett gemensamt utgångsvärde för användning i resp. enhet,
- att synkroniserat och periodiskt uppräkna ett räknevärde hos vardera enheten,
- att vid vardera enheten, oberoende av varandra, generera en nyckel utifrån utgångsvärdet samt räknevärdet och
- att använda denna sålunda genererade nyckel vid autenticeringen.

Detta förfarande är för övrigt precis det som förmodligen många av oss använder när vi kommunicerar med vår bank el. dyl. - Mot bakgrund av teknikens ståndpunkt enligt patentskriften hävdar vi att det nu aktuella patentkravet inte ens är nytt och därför inte patenterbart. Skulle Patentbesvarsrätten finna att det föreligger någon avvikelse, vilket vi inte kan finna, hävdar vi med bestämdhet att patentkravet är närliggande för fackmannen i jämförelse med patentskriften och därför inte patenterbart.

D6

Vi har försökt att hitta ytterligare skriftlig information om "notoriskt kända förfaranden". Detta är svårt eftersom det rör gammal kunskap som normalt ingen skriver om idag. Vi har emellertid i en doktorsavhandling från universitetet i Linz av Dipl.-lng. Otto J. Horak /…/ funnit en redogörelse för nyckelmodifikation som bl.a. behandlar så gamla system som Caesar-chiffer. Här står på sidan 183 som gammal känd teknik att man kan utföra manuella nyckelförändringar varvid man utgår från en för längre tid giltig basnyckel [=utgångsvärde] och skapar en arbetsnyckel (t.ex. en dagsnyckel). Uträkningen av ny arbetande nyckel sker genom en mellan kommunikationsparterna avtalad omräkning med hjälp av data som är kända för dem båda. På detta sätt sker en oberoende, parallell framräkning av en ny arbetsnyckel hos vardera kommunikationsparten. Med stöd av doktorsavhandlingens redogörelse för "gamla kända förfaranden" hävdar vi att patentet inte omfattar en patenterbar uppfinning. ---

I D6 på sidan 183, 12 rader nerifrån, står "Manuelle Schlüsselmodifikationen, die aus einem, für längere Zeit gültigen Grundschlüssel einen Arbeitsschlüssel (z.B. Tagesschüssel) machten, bestanden aus vereinbarten Umrechnungen mit Hilfe von Parametern, bestehend aus Daten, die beiden Kommunikationspartnern bekannten waren. Solche Daten konnten, etwa die Frequenz der Funkverbindung, des Tagesdatum oder ähnliche Werte sein". - Detta blir i vår översättning: "Manuella nyckelförändringar som framställde en arbetsnyckel (t.ex. en dagsnyckel) från en för längre tid giltig grundnyckel [[=utgångsvärde]] bestod av överenskomna omräkningar med hjälp av parametrar som består av data som är kända för båda parter. Sådana data kan vara av typen radiofrekvensen, datum eller liknande värden." - Att detta innebär att man gör nyckelomräkningen oberoende och parallellt, dvs. skapar en ny arbetsnyckel vid båda parter, är självklart och kräver inte mycket fackmannamässig bakgrund för att förstå. Skulle endast en part göra en nyckelomräkning och på något sätt överföra den omräknade nyckeln till den andra parten (vilket ju alla tidigare resonemang i detta ärende understrukit är förödande och helt otänkbart) skulle ju allt tal om "överenskomna omräkningar med hjälp av parametrar som består av data som är kända för båda parter" vara helt obegripligt. I ett sådant (helt otänkbart) förfarande behöver naturligtvis inte den som inte skall räkna ut någon ny nyckel vara informerad om vare sig parametrarna eller den algoritm som skall användas vid omräkningen. - Det är i stället fullständigt klart att omräkningen sker oberoende och parallellt hos vardera kommunikationsparten och därmed är principen för patentets huvudkrav helt känd. ---

Andrahandsyrkandet

Tillägget till de självständiga patentkraven enligt patentet innebär att det uttryckligt anges att det initialt sker en synkronisering och därpå endast synkronisering vid behov. Redan i invändningsskriften har vi påpekat angående det dåvarande patentkravet 4 att det aktuella synkroniseringsförfarandet - följesynkronisering - är ett välkänt synkroniseringsförfarande i sig och att användningen i detta sammanhang inte kan medföra att ett annars icke patenterbart förfarande blir patenterbart. ---

D9

En fackman på kryptoområdet sysslar med såväl kryptering som autenticering. Han är således förtrogen med båda frågorna som båda berör en säker och hemlig överföring av information. I ett läge där det är känt eller närliggande för denne fackman - i jämförelse med envar av D1, D2, D2', D5 och D6 och notoriskt kända blankettchifferförfaranden - att utföra krypterad överföring på det sätt som anges i de självständiga patentkraven i första- och andrahandsyrkandena och likaledes känt eller närliggande för denne fackman - i jämförelse med D5 - att utföra autenticering enligt samma patentkrav, är det uppenbart närliggande att utföra båda de kända förfarandena på samma sätt, så fort ett önskemål om samtidig autenticering och kryptering har inställt sig. Detta måste vara den första tanke som infinner sig hos fackmannen.

Vi har här fört ett resonemang utan att blanda in någon ytterligare skrift. Genom en närliggande kombination av exempelvis D5 och D6 föregriper man de självständiga patentkraven i tredje- och fjärdehandsyrkandena. - Att det är närliggande för fackmannen att samtidigt och med samma nyckel autenticera och kryptera ett meddelande är emellertid förut känt i sig och visas bl.a. i D9. Vi har valt att visa detta med ytterligare en lärobok - även D1 och D2 är läroböcker - eftersom det tydligt visar att patenthavaren söker patentera grundläggande förfaranden som ingår i den kunskap alla fackmän på kryptoområdet besitter, vilket en lärobok kan sägas vara en avspegling av.

I kapitel 9 i D9 diskuteras hashfunktioner och dataintegritet och en fyllig presentation av auteticering ur olika aspekter presenteras, såväl "data integrity" som det vidare begreppet "data origin authentication", se speciellt sidan 361. I inledningen på sidan 321 och vidare på sidan 323 definieras hashfunktioner av typen MDC och MAC. - Kapitel 9.6 går sedan närmare in på olika sätt att autenticera och vi pekar på figuren 9.8 på sidan 360 där 9.8(a) visar ren autenticering med hjälp av en MAC, som ett invärde har en "secret key", vilket motsvarar en "session key" eller en arbetande nyckel dvs. den nyckel som bl.a. kan skapas av ett förfarande enligt patentet. Delfiguren 9.8(b), visar autenticering med samtidig kryptering av meddelandet med samma "secret key"."session key" eller arbetande nyckel, se också huvudfigurtextens avslutning: "The second method provides encipherment simultaneously". Här visas således att man med samma nyckel såväl autenticerar som krypterar ett meddelande.

Beskrivningen av förfarandena utvecklas i kapitlet 9.6.5 som heter "Data integrity combined with encryption". På sidan 365 under punkten (ii) redögors närmare för det som visas i figur 9.8(b). – Notera att vi har anfört det ovanstående för att visa att det är känt att använda samma nyckel för att såväl autenticera som kryptera och dessutom i samma förfarande. Vi har inte hävdat att det här skulle stå att den använda nyckeln här skulle vara framställd enligt

patentet. Det är själva kopplingen att använda samma nyckel för såväl autenticering som kryptering vi har visat.

Den "secret key"="session key"=arbetande nyckel som sedan används kan vara av vilken som helst i och för sig känd typ. För fackmannen är det enligt tidigare resonemang känt eller närliggande att skapa nycklar på det patenterade sättet mot bakgrund av kunskap från envar av D1, D2, D2', D5, D6 och notoriskt kända blankettchifferforfaranden. Kryptofackmannen är samtidigt den fackman som har att lösa frågan om autenticering och det är för honom en närliggande kombination av något av det ovanstående med kunskapen om samtidig autenticering och kryptering enligt D9 som leder fram till tredje- och fjärdehandsyrkandena och därmed förtar uppfinningshöjden för dessa.

Ericsson har till utveckling av sin talan anfört i huvudsak följande.

Förstahandsyrkandet

D3 visar en metod för krypterad överföring mellan åtminstone två enheter i ett datakommunikationssystem via en osäker kommunikationskanal i ett Bluetooth-system. Datakommunikationssystemet enligt det självständiga systemkravet kan vara Bluetooth vilket nämns i patentets beskrivning på sid. 5, rad 28 som det enda konkreta exemplet på ett system där den angivna uppfinningen kan användas. - På sidan 177 i D3 visas steget att komma fram till ett gemensamt utgångsvärde, dvs. utgångsvärdet Kc genom initieringsprocedur som i D3 kallas E3. - Från figur 14.4 sid. 160 i D3 visas att utgångsvärdet motsvaras av Kc, räknevärdet av clock och att payload key generator genererar en payload key som motsvarar den genererade nyckeln.

Från figur 14.4 sid. 160 i D3 tillsammans med avsnitt 9.1 sid 87 visas att alla Bluetooth-enheter, dvs. master och slav som etablerar en kommunikationslänk synkroniserar sina klockor genom att en del av masterklockans värde, dvs. "clock" sänds till slaven under etablering av förbindelsen. Se sid. 48, första stycket samt avsnitt 4.2.3 på sid. 49. Detta värde, clock, tillsammans med kontinuerliga accesskoder med synkroniseringsinformation (fig. 4.2 sid. 48) innebär att varje slav i förbindelse med en master är synkroniserad. Räknevärdet motsvarar alltså ett värde, "clock", från masterklockan som räknas upp synkroniserat. Alltså visas steget att synkroniserat och periodiskt uppräkna ett räknevärde hos vardera enheten.

Från figur 14.4 sid. 160 i D3 visas att en nyckel "payload key" genereras vid vardera enheten utifrån utgångsvärdet Kc samt räknevärdet clock. Master och slaven har sina respektive klockor som tickar på oberoende av varandra, mer specifikt rumsoberoende av varandra. - I figur 14.4 sidan 160 i D3 visas att de genererade nycklarna används vid en efterföljande krypterad överföring. - Vi vill påpeka att det endast är synkroniseringsinformation som utbyts kontinuerligt i D3 och att inget utbyte av krypteringsinformation (dvs. nycklar) sker.

D4 är en metod för kryptering i ett GSM-system. GSM-systemet innefattar kommunikation mellan åtminstone två enheter via en osäker kanal.

SE 517 460, krav 1:
omfattande stegen att:
-vid en initieringsprocedur komma fram till ett gemensamt utgångsvärde för användning i respektive enhet;
Från figur C.2 sid. 49 tillsammans med avsnitt C.0 sid. 48 i D4 visas steget att

komma fram till ett gemensamt utgångsvärde Kc genom initieringsprocedur A8.

SE 517 460, krav 1:
-synkroniserat och periodiskt uppräkna ett räknevärde hos vardera enheten;
I D4 på sidan 49, tredje stycket, visas att ett räknevärde hos vardera enheten uppräknas synkroniserat och periodiskt genom räknevärdet COUNT som beräknas från ett TDMA ramnummer (frame number). Dvs., TDMA ramarna är synkroniserade och COUNT räknas upp för varje ny ram som skickas.

SE 517 460, krav 1:
-vid vardera enheten, oberoende av varandra, generera en nyckel utifrån utgångsvärdet samt räknevärdet; och
I figur C.2 sidan 49 i D4 visas att en nyckel BLOCK1 genereras vid vardera enheten, oberoende av varandra (dvs. rumsoberoende av varandra), utifrån utgångsvärdet Kc samt räknevärdet COUNT.

SE 517 460, krav 1:
-använda dessa sålunda genererade nycklar vid en efterföljande krypterad överföring eller autentisering.
I figur C.2 sidan 49 i D4 visas att de genererade nycklarna används vid en efterföljande krypterad överföring.

Således är stegen enligt patentkrav 1, enligt förstahandsyrkandet, förut kända genom D3 men också genom D4. - Metoden enligt patentkrav 1 uppvisar därför ingen nyhet mot vare sig D3 eller D4 och är således ej patenterbar.

Andrahandsyrkandet

Kravet 1 enligt andrahandsyrkandet som är en sammanslagning av krav 1 och 4 är inte heller nytt, eftersom:
i krav 4 anges att räknarna endast utför kompletterande synkroniseringssteg vid behov. Enligt sid. 3 rad 31-37 och sid. 6, rad 20-26 av beskrivningen betyder synkroniseringssteg att en synkronisering sker när tex. räknevärden utbyts medan synkroniseringstest innebär att en kontroll görs huruvida ett synkroniseringssteg är nödvändigt, dvs. om det finns ett behov för synkronisering.
I D3 sid 87, avsnitt 9.1, visas att Bluetooth uppdaterar (= utför ett synkroniseringssteg) sin räknare, dvs. master clock då klockorna drivit en viss tid i förhållande till varandra, dvs. endast vid behov. Ett synkroniseringstest utförs visserligen kontinuerligt i D3 men synkroniseringssteg utförs endast vid behov. Synkroniseringstestet förklaras inte alls i patentet, dvs hur det går till eller hur ofta det utförs. Det finns därför inget som utesluter att det kan göras kontinuerligt.

Det som anges i patentkrav 1 enligt andrahandsyrkandet är således ej nytt i förhållande till D3.

Tredje- och fjärdehandsyrkandet

D3 visar enligt ovan en metod för krypterad överföring där ett nyckelvärde genereras baserat på ett utgångsvärde och ett räknevärde som räknas upp periodiskt och synkroniserat. Dessutom visas i D3 att ett synkroniseringssteg kan utföras vid behov. - Från D7, RFC 2246, visas en metod för kryptering och autentisering där en nyckel genereras som används för både kryptering och autentisering. I D7, sektion 6.2.3 beskrivs hur meddelanden ("data records") som

utbytes mellan två enheter skyddas med hjälp av kryptering och integritetsskydd (autentisering av meddelanden). Integritetsskyddet utgörs av en s.k. "Message Authentication Tag" som beräknas över klartexten med hjälp av en hemlig nyckel, "MAC-nyckel". Vidare beskrivs hur meddelanden samtidigt skyddas med hjälp av kryptering. Kryptering kan ske med hjälp av ett block eller ett strömchiffer. I båda fallen används en krypteringsnyckel. Vidare i sektion 6.3 i D7, beskrivs hur MAC-nyckeln och krypteringsnyckeln beräknas utifrån en gemensam hemlighet/nyckel, den s.k. "master secret", och andra gemensamma värden så som slumptal.

För att visa att uppfinningen saknar uppfinningshöjd används "problem-solution-approach" (problem-lösningsmetoden). - D3 anses vara närmast kända teknik, eftersom den avser en metod för kryptering enligt krav 1, enligt tredje-och fjärdehandsyrkandena. - Skillnaden mellan det som visas i D3 och det som anges i de självständiga kraven enligt tredjehandsyrkandet respektive fjärdehandsyrkandet är att samma nyckel ej används för autentisering och kryptering. Autentisering innebär att den sändande och mottagande kan identifiera sig för den andra, dvs. mottagare och sändare kan säkerställas.

Den tekniska effekt som uppnås med hjälp av den här skillnaden är att den krypterade och överförda trafiken integritetsskyddas, dvs. man kan säkerställa mottagare och sändare. - Det objektiva problemet blir då att tillhandahålla en metod med ökad säkerhet, där sändare och mottagare kan identifieras. - Om man utgår från D3 och vill lösa det objektiva problemet är det uppenbart för en fackman att inte enbart använda den genererade nyckeln för kryptering utan även för autentisering. Detta är speciellt uppenbart om man beaktar D3 tillsammans med , eftersom D7 visar en metod där en genererad nyckel används för både kryptering och autentsiering.

De självständiga kraven, enligt tredjehandsyrkandet och fjärdehandsyrkandet, saknar uppfinningshöjd i ljuset av D3 i kombination med D7. Följaktligen skiljer sig inte de självständiga kraven enligt tredjehandsyrkandet och fjärdehandsyrkandet väsentligen från det som är tidigare känt.

Som grund för denna överklagan åberopar vi även att patentet SE 517 460 avser en uppfinning som inte är så tydligt beskriven att en fackman med ledning av beskrivningen kan utöva uppfinningen. - I beskrivningen, tex. på sidan 3, rad 10 och rad 25, sägs att en nyckel genereras i vardera beräkningsenhet, oberoende av varandra och på sidan 3, rad 7-20, beskrivs hela tillvägagångssättet med att ta fram nyckeln som kan användas för kryptering/autentisering. - Uttrycket "oberoende av varandra" förekommer i alla självständiga krav enligt l-4:e handsyrkandena. - Detta uttryck får anses vara så otydligt beskrivet så att det inte är möjligt för en fackman att utöva uppfinningen med ledning av beskrivningen.

Om man studerar de tre sista stegen i krav 1:
-synkroniserat och periodiskt uppräkna ett räknevärde hos vardera enheten;
-vid vardera enheten, oberoende av varandra, generera en nyckel utifrån utgångsvärdet samt räknevärdet; och
-använda dessa sålunda genererade nycklar vid en efterföljande krypterad överföring eller autentisering.
finner man att man har ett räknevärde i vardera enheten som räknas upp. Eftersom det sker synkroniserat så måste varje enhet ha samma värde vid varje tidpunkt. Nycklar baserade på detta räknevärde genereras vid mottagaren och sändaren och dessa nycklar används sedan för att kryptera/dekryptera en

överföring. Nycklarna som generas måste vara baserade på samma räknevärde, vilket innebär ett tidsberoende, eftersom räknevärdet varierar i tiden. Dvs. det måste vara samma nyckel som genereras i vardera enheten som används för kryptering om en dekryptering av den krypterade överföringen ska kunna ske. Om de inte är baserade på samma räknevärde så måste en synkronisering ske för att kryptering respektive dekryptering ska fungera.

Vidare finns ett ytterligare beroende eftersom att vardera enhet måste initialt laddas med ett gemensamt utgångsvärde. Eftersom utgångsvärdet är ett gemensamt värde så innebär det att en initial synkronisering i själva verket sker eller åtminstone ett utbyte av information. Detta är tvärtemot av vad som framgår på sidan 7, rad 19, där det står att ingen information utbyts. Detta utgångsvärde används enligt ovan för att generera nycklarna. - Det innebär att "oberoende av varandra" ej kan tolkas som tidsoberoende eller nyckeloberoende. Vilket slags oberoende som avses framgår inte av beskrivningen. En fackman kan därför inte med hjälp av beskrivningen ledas till hur nycklarna ska kunna genereras *oberoende av varandra.* - Dessutom framgår det inte från beskrivningen hur ett synkroniseringstest respektive synkroniseringsteg skall utföras. - Enligt sid. 3, rad 31-37 och sid. 6, rad 20-26, betyder synkroniseringssteg att en synkronisering sker när tex. räknevärden utbyts medan att synkroniseringstest innebär att en kontroll görs huruvida ett synkroniseringssteg är nödvändigt, dvs. om det finns ett behov för synkronisering.

Själva synkroniseringstestet förklaras inte alls i patentet, dvs. hur det går till eller hur ofta det utförs. Därför finns inget i patentet som utesluter att detta synkroniseringstest kan göras kontinuerligt. Synkroniseringssteget exemplifieras med att ett utbyte av räknevärden sker. Det nämns i beskrivningen (liksom i de självständiga kraven enligt andrahandsyrkandet och fjärdehandsyrkandet) att ett synkroniseringsteg sker vid behov. För att det ska kunna ske vid behov och ske före nyckelgenereringen så måste man först identifiera det behovet, i form av ett synkroniseringstest, så som det indikeras i fig. *2,* steg S6. Dessutom beskrivs det ingenstans i beskrivningen hur ett sådant synkroniseringstest kan gå till. - Det bör noteras att trots att patenthavaren har fått ett flertal tillfällen att klargöra begreppet "oberoende av" så har inga sådana klargöranden gjorts. - En fackman inom området kan därför inte med ledning av beskrivningen utöva uppfinningen.

Vidare vill vi repetera från den muntliga förhandlingen av den 30 maj att PRV:s avslagsbeslut daterat 2003-12-12 är mycket dåligt underbyggt med följande motiveringar:
PRV:s beslut grundar sig inte på uppfinningen såsom den anges i de självständiga kraven. Beslutet grundar sig på en egen tolkning av kraven, en tolkning som inte helt finner stöd i beskrivningen. Dessutom anger PRV skillnader mot D3 och D4 som inte framgår av kraven eller beskrivning, t.ex. avståndsaspekten. Exempelvis anger PRV att D3 inte behandlar samma område eftersom tekniken enligt D3 endast skulle kunna användas för korta avstånd. Vidare avfärdar PRV D3 som ett icke utgörande hinder, "då en fackman som tar del av D3 inte skulle ledas till att konstruera ett system för överföring av information mellan två enheter på ett större avstånd". Tvärtemot PRV:s uppfattning, så anges i beskrivningen till det omtvistade patentet att uppfinningen är applicerbar på Bluetooth, dvs. även vid korta avstånd. Vad uppfinningen enligt kraven avser är vad som händer i respektive sändarenhet och mottagarenhet, oavsett avstånd mellan dessa enheter. Avståndsresonemanget måste därför avfärdas som helt irrelevant eftersom kravet inte anger några avståndsbegränsningar. - Vi vill även bemöta PRV:s påstående att Bluetooth inte är avsett för överföring av textmeddelande (såsom metoden och systemet enligt patentet), utan endast är avsett för överföring av tangenttryckningar och musrörelser. Detta påstående är felaktigt. Bluetooth är avsett att

stödja datakommunikation mellan två enheter där data inbegriper tex. överföring av textfiler, SMS, MMS, etc. Dessa enheter kan vara två datorer, två mobiltelefoner, en mobiltelefon och en dator, osv.

Patenthavaren har till utveckling av sin talan framhållit bl.a. följande till stöd för uppfinningens patenterbarhet.

Tolkning av kravterminologi

Den tolkning av kraven, och de termer som används i kraven, som gjorts av Patentverket under invändningsförfarandet, och som ligger till grund för beslutet, har ifrågasatts av båda invändarna. Dessa påståenden förefaller dock fullständigt grundlösa. Tvärtom måste den tolkning som tidigare gjorts anses fullständigt rimlig då kraven läses i ljuset av patentet i övrigt. [I] detta sammanhang hänvisas till Artikel 69 EPC, vilken äger motsvarighet i svensk lag, där det uttryckligen anges att beskrivningen skall vara vägledande vid tolkningen av termer definierade i patentkraven. Specifikt säger nämnda Artikel 69 bl a följande:
"(1) The extent of the protection conferred by a European patent or a European patent application shall be determined by the terms of the claims. Nevertheless, the description and drawings shall be used to interpret the claims. "

Nyhet

Kombinationen av alla de särdrag som anges i patentkrav 1 respektive patentkrav 8 framgår inte av något av de av invändarna anförda dokumenten D1, D2, D2', D3, D4, D5 eller D6, och därmed har uppfinningen enligt patentet nyhet. ---

I D1 förefaller hänvisningen speciellt avse stycket 7.2 (sid. 139-152), där det diskuteras nyckelhantering i olika kända system, såsom t ex DES. I stycket 7.2.2 (sid. 145-147) omnämns specifikt hur nycklar genereras och överförs mellan de kommunicerande enheterna. Därvid konstateras det inledningsvis initialt att nycklar inte öppet kan sändas mellan enheterna, men lösningarna som anvisas på detta problem är helt andra än hos uppfinningen enligt patentet. Lösningar som diskuteras är t ex att skicka ut nycklarna via andra kanaler eller i olika delar, eller att använda så kallade allmänna nycklar. Den uppfinningsenliga lösningen att vid vardera enheten, oberoende av varandra, generera den nyckel som skall användas är dock inte beskriven. - I stycket som diskuterar standarden X 9.17 diskuteras också endast genererande av nycklar vid en enhet, och det finns inget som indikerar att ett samtidigt, oberoende genererande av nycklar vid flera enheter är avsett. Det finns inga som helst belägg för det påstående som görs av invändaren, att en fackman som läst D1 före prioritetsdagen för patentet skulle ha läst in något ytterligare i beskrivningen av D1 än vad där faktiskt står. Tvärtom anvisar D1 många alternativa lösningar för hur de vid en enhet genererade nycklarna på ett säkert vis, t ex via alternativa kanaler, kan överföras mellan olika enheter.

Följaktligen skiljer sig uppfinningen såsom den definieras av patentkraven 1 resp. 8 från det som beskrivs i D1, åtminstone genom att D1 inte beskriver något periodiskt uppräknande av ett räknevärde vid olika enheter eller något oberoende genererande av nycklar vid respektive enhet. --- Snarare förefaller t ex diskussionen under stycke 7.2.2 peka i motsatt riktning, och därmed bort från den aktuella uppfinningen. Åtminstone av dessa skäl skiljer sig därmed den aktuella uppfinningen från D1. ---

Vad gäller D2 och D2' har hänvisning primärt skett till stycket 8.2 på sid. 292-302. I stycke 8.2.2 hänvisas till en lösning med s k meddelandenycklar, vilka överförs mellan enheter och tillsammans med basnycklar hos respektive enhet bildar den fullständiga nyckeln som används vid krypteringen.

Lösningen som beskrivs i D2/D2' kräver normalt att synkroniseringsinformation, och speciellt meddelandenycklar, kontinuerligt överförs mellan enheterna i samband med varje överföring. Dock kan även tillfälliga avbrott i denna överföring hanteras med s k flywheeling, genom att meddelandenycklar inte är slumpmässiga, utan är härledbara bakåt och framåt utifrån redan överförda meddelandenycklar. - /…/ Det kan dock i sig anses diskutabelt om de meddelandenycklar som diskuteras i D2/D2' kan sägas utgöra ett räknevärde i patentets mening. Vidare beskriver D2/D2' en lösning där det i normalfallet sker en kontinuerlig överföring av synkroniseringsdata mellan enheterna, och utan något oberoende uppräknande av räknevärden vid respektive enhet för användning vid generande av nycklar.

I de undantagsfall då "flywheeling" används sker inte heller något oberoende synkroniserat och periodiskt uppräknande hos respektive enhet. Tvärtom är det detta som är själva poängen med flywheeling, nämligen att se till att en enhet som misslyckats med att ta emot synkroniseringsinformation och som därmed kommer ur fas (dvs blir osynkroniserade) i efterhand (dvs varken synkroniserat eller periodiskt) försöker generera nycklar för att förstå mottagen information som den ej lyckats tillgodogöra sig. Detta är dock ej den funktion som definieras i patentet. - Vidare används flywheeling enligt D2/D2' endast i undantagsfall, medan man i normalfallet använder sig av den kontinuerliga utsändandet av synkroniseringsinformation. Enligt uppfinningen som definieras i patentet används däremot i normalfall det oberoende uppräknandet och nyckelgenererandet, medan utbytande av synkroniseringsinformation endast sker i undantagsfall. Det finns överhuvudtaget ingen beskrivning i D2/D2' av att använda flywheeling som ett alternativ till det kontinuerliga utsändandet av synkroniseringsdata. Det enda som beskrivs i D2/D2' är att använda flywheeling som ett komplement till utsändandet av det kontinuerliga utsändandet av synkroniseringsdata, för att hantera kortvarigt avbrott i kommunikationen, där alltså utsänd synkroniseringsdata inte kommer fram. Flywheeling kan därmed inte anses utgöra något synkroniserat och oberoende generande av en nyckel vid olika enheter i patentets mening. ---

Även D2 och D2' skiljer sig från den aktuella uppfinningen åtminstone i det att dessa dokument inte beskriver ett synkroniserat och periodiskt uppräknande av ett räknevärde i respektive enhet, och ett efterföljande oberoende genererande av nycklar i vardera enheten. Tvärtom bygger nyckelgenererandet i de utföranden som diskuteras i dessa dokument på att information överförs mellan enheterna. Den aktuella uppfinningen är därmed ny även i förhållande till D2 och D2'.

D3 beskriver en teknik där synkroniseringsinformation som ska användas vid nyckelgenererandet hela tiden kontinuerligt överförs mellan enheterna. Därmed kan D3 inte anses beskriva något synkroniserat och periodiskt uppräknande av ett räknevärde vid vardera enheten, och inte heller att nycklar genereras oberoende av varandra vid respektive enhet. Den aktuella uppfinningen bygger på att nycklar genereras i vardera enheten utifrån endast räknevärde och utgångsvärde, och att detta inte kräver någon kommunikation mellan enheterna, varken kontinuerligt eller inför varje nyckelgenerering. På detta sätt blir nyckelgenererandet oberoende vid respektive enhet, vilket har uppenbara fördelar med avseende på säkerhetsnivå och kostnadseffektivitet, såsom diskuterats tidigare. I tekniken

enligt D3 krävs däremot ett ständigt och kontinuerligt informationsutbyte av synkroniseringsinformation mellan enheterna. Sålunda måste den aktuella uppfinningen anses vara ny i förhållande till D3. ---

Dokumentet D4 avser kryptering inom GSM-systemet. Detta system liknar i stor utsträckning det som ovan diskuteras utifrån D3. I systemet enligt D4 sker likaledes en kontinuerlig synkronisering, i form av ständigt utsändande av ett räknevärde ("count"). Följaktligen använder inte heller den lösning som presenteras i D4 någon synkroniserad och periodisk uppräkning av ett räknevärde hos vardera enheten, eller något efterföljande oberoende genererande av en nyckel vid vardera enheten. Tvärtom anvisar D4, liksom D3, ett ständigt och kontinuerligt utbyte av synkroniseringsinformation, varvid något oberoende uppräknande och nyckelgenererande inte kan sägas ske. - Följaktligen skiljer sig uppfinningen såsom den definieras av patentkraven 1 och 8 även från det som beskrivs i D4, och uppvisar därmed nyhet i förhållande till detta dokument.

Dokumentet D5 avser en anordning för skapande av en oförutsägbar kod enligt en algoritm, varvid algoritmen räknar ut den oförutsägbara koden baserat på en statisk variabel och ett tidsvärde. Den sålunda genererade koden skickas sedan till en andra enhet, där den jämförs med en på liknande sätt genererad kod hos denna enhet, varvid identifiering mellan enheterna kan ske (se t ex sammandraget på sid. 1). Det statiska värdet är typiskt en PIN-kod som matas in av användaren. - Dokument D5 avser dock inte någon krypterad överföring eller krypterad autentisiering på det sätt som definieras i patentkrav 1 och 8 hos patentet. Istället överförs enligt D5 den genererade oförutsägbara koden direkt och öppet mellan enheterna. Någon kryptering omnämns i D5 över huvud taget inte, och speciellt inte någon kryptering som använder den oförutsägbara koden som nyckel.

Den oförutsägbara koden enligt D5 kan möjligen anses likna den nyckel som genereras enligt patentet. Denna nyckel enligt D5 kan dock i så fall inte anses användas vid en efterföljande krypterad överföring eller autentisiering på det sätt som definieras enligt patentet. Istället sker identifieringen enligt D5 genom överföring av den skarpa nyckeln. Detta är helt oförenligt med det som definieras enligt patentet. Detta är uppenbart, speciellt som kraven skall tolkas i ljuset av beskrivningen, där det utom allt tvivel framgår att ett syfte med uppfinningen enligt patentet är att undvika att de genererade nycklarna överförs via den osäkra kanalen. Detta framgår t ex på sid. 7, rad 21-28 hos patentet, där uppfinningen diskuteras allmänt och inte enbart med avseende på någon specifik utföringsform, och i bakgrundsbeskrivningen, där problemet med överförande av nycklar speciellt diskuteras.

Det enda som enligt patentet är ämnat att överföras mellan enheterna via den osäkra kanalen är ett räknevärde, och detta är vidare endast att ske för att utföra kompletterande synkronisering, och endast då detta är påkallat på grund av att enheterna befunnits vara osynkroniserade relativt varandra. Någon sådan kompletterande synkronisering diskuteras dock över huvud taget inte i D5. - Det kan därmed konstateras att systemet som beskrivs i D5 på några avgörande punkter skiljer sig från den uppfinning som definieras i patentet, och därmed även går tvärt emot det grundläggande syftet som ligger bakom patentet.

Invändare 1 anför att s k "notoriskt kända förfaranden" skulle vara nyhetsförstörande för uppfinningen. Det kan dock inledningsvis konstateras att denna argumentation huvudsakligen bygger på lösa antaganden och påståenden som på inget sätt har stöd i anförda skrifter. Det som diskuteras i D6 tillför i detta

sammanhang inget i sak. ---

D6 beskriver, i den del som Invändare 1 hänvisar till, ett manuellt förfarande, och avser sålunda inte krypterad överföring eller autentisering i ett datakommunikationssystem. Noterbart är också att D6, i det sista stycket på sid. 183 snarare pekar bort från den aktuella uppfinningen, då det tydligt sägs att det manuella systemet inte anses lämpat för datoriserade system. Vidare kan D6 inte anses beskriva ett periodiskt och synkroniserat uppräknande av räknevärden vid respektive enhet. Sålunda måste den aktuella uppfinningen, av åtminstone dessa skäl, även anses uppvisa nyhet gentemot D6.---

Vidare kan det konstateras att dessa "kända" förfaranden, i den mån de är verifierbara, avser mycket gammal teknik, som använts för helt andra typer av överföring, för helt andra syften och för överföring på helt andra typer av kommunikationsvägar. Det kan därför starkt ifrågasättas om dessa förfaranden över huvud taget kan anses ha någon relevans när det gäller att bedöma uppfinningen enligt patentet.

Den ålderdomliga teknik med blankettchiffer som diskuteras av Invändare 1 omfattar vidare en uppsättning redan färdiggenererade nycklar, där man sedan i viss ordning väljer vilka nycklar skall använda. Denna manuella hantering skulle dock vara synnerligen opraktiskt för modern datakommunikation.

Uppfinningen enligt patentet skiljer sig sålunda på många avgörande punkter från de "notoriskt kända förfarandena" som Invändare 1 diskuteras, t ex genom att inget periodiskt och synkroniserat uppräknande av ett räknevärde sker, att nycklar oberoende genereras vid olika enheter baserat på räknevärde och utgångsvärde och att överföringen avser krypterad överföring och autentisiering i ett datakommunikationssystem. - Den enda beröringspunkten mellan de anförda förfarandena och uppfinningen förefaller vara att de båda på något sätt involverar kryptering. Att kryptering i sig är känt, och även har använts under lång tid har dock aldrig ifrågasatts av patenthavaren.

Det kan också allmänt konstateras att, tvärt emot de påståenden som görs av Invändare 1, användning av en mycket gammal teknik som finner ny användning i ett helt nytt sammanhang, normalt snarare kan anses vara en klar indikation på att erforderlig uppfinningshöjd måste anses föreligga, än ett bevis på motsatsen. Speciellt gäller detta när den gamla tekniken i det nya sammanhanget ger oväntade fördelar och förutsatt att tekniska medel för åtgärden funnits under lång tid utan att någon för den skull har gjort detta tidigare. - Med andra ord kan det konstateras, att om det, såsom Invändare 1 påstår, verkligen skulle ha varit möjligt och närliggande att överflytta teknik som varit känd sedan 1800-talet till moderna datakommunikationssystem, så borde detta givetvis ha gjorts långt tidigare. Att så inte är fallet är en tydlig indikation på att uppfinningen enligt patentet inte kan anses föregripas av de omtalade "notoriskt kända" förfarandena. ---

Det har noterats att ingen av skrifterna D7-D9 av invändarna i sig själva har ansetts förta nyheten för de aktuella patentkraven, och någon djupare diskussion av dessa dokument kommer därmed inte att ske i detta sammanhang.

Sålunda kan det konstateras att den aktuella uppfinningen, såsom den definieras i patentkraven enligt förstahandsyrkandet, måste anses uppfylla kraven på nyhet gentemot den anförda kända tekniken.

[Uppfinningshöjd]

Uppfinningen såsom den definieras enligt förstahandsyrkandet måste också anses uppvisa erforderlig uppfinningshöjd gentemot de anförda skrifterna, och vilka som helst kombinationer av dessa.

Uppfinningen avser en metod och ett system för en säker krypterad överföring eller autentisiering mellan åtminstone två enheter via en osäker kommunikationskanal, vilket allmänt kan sägas gälla även de anförda skrifterna, liksom många andra kända lösningar. Dock avses det i föreliggande uppfinning specifikt att lösa problemet att åstadkomma ett relativt enkelt och kostnadseffektivt system, där samtidigt säkerheten hålls på en relativt hög nivå. Detta problem löses enligt uppfinningen genom att minska informationsutbytet mellan enheterna, vilket i sin tur möjliggörs genom att synkroniserat och periodiskt uppräkna räknevärden hos vardera enheten, och att använda räknevärdena för att i enheterna, oberoende av varandra, generera nycklar för användning vid autentisering/kryptering. Härigenom behöver nycklar aldrig överföras, och synkroniseringsinformation avseende räknevärdet behöver endast i undantagsfall utbytas mellan enheterna, och även när detta är påkallat innehåller sådan överförd synkroniseringsinformation ingen del av nyckelinformationen. Jämfört med känd teknik möjliggör uppfinningen sålunda datakommunikation med förbättrad säkerhet och/eller mindre krävande och mer kostnadseffektiv överföring, med t ex möjlighet att använda kortare nycklar och enklare kryptering, men under bibehållande av samma eller bättre grad av säkerhet.

Oavsett vilket av de ovan diskuterade dokumenten som används som betraktas som närmast, så finns det inget av dessa dokument som konkret diskuterar detta problem, eller någon lösning på detsamma. Vidare är det inget av dessa dokument som pekar i riktning mot den aktuella uppfinningen för lösande av något likartat problem.

Sålunda beskrivs den uppfinningsenliga lösningen inte i något av de anförda dokumenten, och någon antydan till denna lösning står överhuvudtaget inte att finna. Följaktligen finns det inget som indikerar att en fackman på området, med kännedom om de anförda skrifterna och i ljuset av det ovannämnda objektiva tekniska problemet, skulle ledas i den riktning som anvisas av patentet. Tvärtom avser alla de anförda skrifterna istället andra, alternativa lösningar, som snarare kan anses leda bort från uppfinningen. Speciellt anvisar t ex D1-D4 som en central del i respektive lösning ett kontinuerligt utbyte av åtminstone synkroniseringsinformation, och D6 antyder tydligt att det diskuterade manuella förfarandet inte är lämpligt för datoriserade miljöer. - Sålunda finns det för det första inga skäl för en fackman på området att i ljuset av det ovan diskuterade problemet vända sig till något av de andra dokumenten, och för det andra finns det inget som indikerar att detta i sa fall skulle ha lett fram till den aktuella uppfinningen. - Uppfinningen enligt patentkrav 1 och 8 hos patentet måste därmed även anses uppvisa erforderlig uppfinningshöjd relativt alla de anförda skrifterna, liksom varje kombination av dessa.

Andrahandsyrkandet

I uppfinningen enligt andrahandsyrkandet är den ytterligare preciseringen införd att enheterna efter en inledande synkronisering av räknarna endast utför kompletterande synkroniseringssteg vid behov. Detta förtydligar därmed ytterligare de ovan diskuterade fördelarna hos uppfinningen som ligger i att utbytet av information rörande krypteringen mellan enheterna kan minimeras. -

Det tillförda särdraget har ingen motsvarighet hos någon av de anförda skrifterna, där det i flera av dem tvärtom är en uttalad förutsätt–ning att synkronisering i princip måste ske kontinuerligt, såsom i D2, D3 och D4. - I denna fråga för Invändare 2 ett mycket märkligt resonemang om att man i D3 och D4 visserligen hela tiden utbyter synkroniseringsinformation och använder denna tillförda information för att kontrollera synkroniseringen hos den mottagande enheten, men att detta inte kan anses vara ett synkroniseringssteg eftersom korrigeringar endast utförs då synkroniseringen visar sig vara felaktig. Detta resonemang är dock mycket teoretiskt, och verkar sakna teknisk förankring.

Ett avgörande moment vid synkroniseringssteget, såsom det diskuteras i den aktuella uppfinningen, är överförandet av synkroniseringsinformation mellan enheterna. Enligt den aktuella uppfinningen, såsom den definieras i andra-handsyrkandet, minskas informationsutbytet genom att synkronisering endast utförs då det är påkallat, och att sålunda synkroniseringsinformation endast vid behov överförs. Detta skiljer sig väsentligt från förfarandena i D3 och D4, där alla väsentliga moment i synkroniseringen utförs regelbundet och kontinuerligt, oav-sett om det finns behov av det eller inte. ---

I D2 är det dock nämnt en möjlighet att hantera tillfälliga avbrott (konceptet med flywheeling som diskuteras i D2). Även i D2 sker dock ingen behovsprövning av synkroniseringen, utan denna förutsätts genomföras så fort möjlighet därtill finns. Därmed är detta särdrag nytt i förhållande till alla de anförda skrifterna. ---

Vad gäller D5 sker över huvud taget ingen synkronisering. Istället förutsätts enheterna ständigt vara synkroniserade, och detta är en förutsättning för att systemet enligt D5 skall fungera. Om enheterna mister sin synkronisering, vilket i praktiken högst sannolikt kommer att ske efter en viss tid blir systemet i princip oanvändbart.

Det kan vidare konstateras att varken D1, D6 eller de påstådda "notoriskt kända" förfaranden som anförs av Invändare 1 innehåller några medel eller steg för att avkänna synkroniseringsstatus eller för att återställa synkroniseringen mellan enheterna vid behov.

Det tillförda accentuerar sålunda skillnaden i det uppfinningsenliga konceptet gentemot de kända lösningarna. Följaktligen måste de nya kraven enligt andrahandsyrkandet även anses uppvisa erforderlig uppfinningshöjd av detta skäl, utöver det som diskuterats med avseende på förstahandsyrkandet.

Tredjehandsyrkandet

I uppfinningen enligt tredjehandsyrkandet är det ytterligare preciserat att metoden/anordningen avser krypterad överföring och autentisering (till skillnad från tidigare kravuppsättningar som avsett krypterad överföring eller autentise-ring).

Den aktuella uppfinningen definierar en metodik som lämpar sig väl för såväl krypterad överföring som autentisering, såsom diskuterats ovan i samband med första- och andrahandsyrkandet, men där speciella fördelar med avseende på enkelhet och effektivitet erhålles då dessa moment utförs samtidigt, men användning av samma nyckelgenereringsförfarande.

Det kan konstateras att de tekniker i D1-D4 och D6 som diskuterats ovan endast

avser krypterad överföring, och att de genererade nycklarna enligt dessa förfaranden inte varken används eller är avsedda för autentisering. Denna tolkning förefaller vidare vara obestridd av invändarna.

D5 avser däremot ett autentiseringsförfarande, där koder genereras och överförs mellan enheter för jämförelse. Detta förfarande är dock varken använt eller avsett för krypterad överföring, och förefaller vidare direkt olämpligt för en sådan användning.

Skrifterna D7 och D9 påstås visa användning av samma nycklar, eller åtminstone väsentligen samma nyckelgenereringsförfarande, för både autentisering och krypterad överföring. Dock beskriver inget av dessa dokument en nyckelgenereringsprocess i enlighet med den aktuella uppfinningen.

Det kan därmed konstateras att den uppfinning som definieras i patentkraven enligt tredjehandsyrkandet även av denna anledning, oaktat det som diskuterats ovan med avseende på första- och andrahandsyrkandena, är nytt i förhållande till den kända tekniken. - Uppfinningen i enlighet med tredjehandsyrkandet måste också anses uppvisa erforderlig uppfinningshöjd gentemot de olika kombinationer av dokument som föreslås av invändarna.

Såsom konstaterats ovan avser D5 en autentiseringslösning som varken är tänkt eller lämpad för krypterad överföring. Del finns inga som helst motiv till varför en fackman inom området, för att åstadkomma en effektivare lösning för krypterad överföring och autentisering skulle ens överväga att försöka kombinera autentiseringsförfarandet enligt D5 med något av de tidigare diskuterade krypteringsförfaranden i D1-D4 och D6. Föreliggande uppfinning måste därmed anses uppvisa erforderlig uppfinningshöjd i ljuset av D5 i kombination med vilket som helst av de andra dokumenten. - Speciellt kan det konstateras att den kombination som lyfts fram av Invändare 1, nämligen D5 + D6, förefaller mycket långsökt, då D5 avser en lösning endast avsedd för autentisering, medan D6 avser en ålderdomlig lösning endast avsedd för krypterad överföring, och som dessutom i D6 själv direkt utpekas som direkt olämplig för datoriserade tillämpningar.

Om vi istället utgår från någon av D1-D4 och D6 som närmast kända teknik kan det objektiva tekniska problemet anses vara att åstadkomma en enklare och mer kostnadseffektiv lösning för krypterad överföring och autentisering, men som ändå ger en adekvat säkerhetsnivå.

I ljuset av detta problem finns det inga skäl till varför fackmannen skulle vända sig till D7 eller D9, eftersom inget av dessa dokument är inriktat på detta. Vidare finns det inget som motivera att en fackman på området skulle ha använt krypteringen/autentiseringen enligt D7 och D9 med de specifika nyckelgenereringsmetoderna enligt D1-D4 och D6 för att lösa detta problem. - Föreliggande uppfinning, såsom den definieras i tredjehandsyrkandet, måste därmed anses uppvisa erforderlig uppfinningshöjd.

Fjärdehandsyrkandet

I uppfinningen enligt fjärdehandsyrkandet preciseras metoden/anordningen enligt uppfinningen med en kombination av de ytterligare särdrag som tillförts i andra- och tredjehandsyrkandena. Den ovanstående diskussionen avseende dessa särdrag är därmed fullt tillämplig även för fjärdehandsyrkandet.

Sålunda definierar patentkraven enligt fjärdehandsyrkandet en metod och

anordning för enkel och effektiv krypterad överföring och autentisering som än tydligare skiljer sig från de ovan diskuterade skrifterna och kombinationer av dessa. Dessa patentkrav uppvisar sålunda nyhet och uppfinningshöjd gentemot dessa skrifter.

Påstått bristande beskrivning av uppfinningen

Invändare 2 framför nu för första gången i sin skrivelse per 15 juni 2007 den ytterligare invändningsgrunden att patentet inte anses beskriva uppfinningen så tydligt att en fackman på området kan utöva den. Skälen till detta skulle vara att uttrycket "oberoende av varandra" såsom det används i patentkraven anses otydligt, samt att detsamma gäller synkroniseringssteget som tagits med i de oberoende patentkraven enligt andra- och fjärdehandsyrkandena.

För det första måste det anses anmärkningsvärt att Invändare 2 har deltagit som invändare i denna process sedan tidigt 2003, då invändningen lämnades in, och först nu, flera år senare, och efter otaliga skriftväxlingar och två muntliga förhandlingar, inser man att man inte förstår uppfinningen och hur den ska realiseras. Bara av detta skäl förefaller denna nya attack på patentet vara helt grundlös.

För det andra kan det konstateras att Invändare 2 förefaller ha missuppfattat de lagstadgade invändningsgrunderna enligt 25 § patentlagen. Patentkraven hos det beviljade patentet i det aktuella ärendet är inte otydliga. Dock är det ingen invändningsgrund att patentkraven hos ett beviljat patent är otydliga, även om så skulle ha varit fallet. Dock kan det för sakens skull påpekas att patenthavaren inte anser att patentkraven hos det beviljade patent är otydliga.

Den invändningsgrund som Invändare 2 nu i detta sena läge har alltså inget med eventuell otydlighet att göra. I stället är den relevanta frågan i detta avseende huruvida patentet i sin helhet kan anses ge en fackman inom området sådan kunskap så att åtminstone något utförande kan utövas utan alltför mycket arbete, och utan att någon uppfinningsförmåga erfordras. Rättsfall från EPO avseende motsvarande invändningsgrund talar om att uppfinningen ska kunna utövas utan "undue burden" (se t ex T 292/85). - I detta fall skulle alltså enligt Invändare 2 en fackman på området inte med ledning av patentskriften i sin helhet kunna komma fram till hur uppfinningen skulle kunna realiseras. Vi har mycket svårt att förstå logiken i detta.

Tvärtom beskriver patentet väl hur nyckelgenereringen kan utföras oberoende i respektive enhet genom att enheterna initieras på samma sätt, genom att räknare uppräknas synkroniserat vid respektive enhet, och att nycklar genereras utifrån ingångsvärdet och det aktuella räknevärdet. På detta sätt krävs ingen ytterligare kommunikation mellan enheterna i samband med nyckelgenererandet, vilket därmed kan ske oberoende vid respektive enhet. En fackman på området skulle inte ha några svårigheter att realisera en sådan lösning. - Vidare beskriver patentet hur behov av synkronisering kan omfatta ett separat synkroniserings-test eller helt enkelt konstaterande av att samma nycklar inte har använts vid ett krypterat meddelande (se t ex sid. 6, raderna 20-29). Båda dessa alternativ är enkla att implementera för en fackman på området. Vidare beskrivs hur synkro-nisering, då behov ansetts föreligga, kan ske genom översändande av aktuellt räknevärde från den ena enheten till den andra (se t ex sid. 7, raderna 19-21). Också detta kan utan några problem realiseras av en fackman på området. Vi anser därmed att patentet i sin helhet beskriver uppfinningen på ett så tydligt sätt att den kan utövas av en fackman inom området.

Bevisning

På begäran av FMV har vittnesförhör hållits med LB.

DOMSKÄL

Utan att ta ställning till frågan om beskrivningen av uppfinningen är så tydlig att fackmannen kan utöva den, konstaterar Patentbesvärsrätten att uppfinningen tillräckligt väl kan förstås av en fackman för att en bedömning av den i patentkraven angivna uppfinningens nyhet och uppfinningshöjd skall kunna göras.

I beskrivningen anges att den räknare och den beräkningsenhet som omfattas av nyckelgenereringsenheterna och som ingår i föredragna utföringsformer av uppfinningen kan vara integrerade i samma enhet samt att denna med fördel kan vara en mikroprocessor. Vidare anges att räknaren med fördel kan styras av en oscillator eller klocka. Det anges också att det är möjligt att utesluta räknare i en eller flera av enheterna, varvid steget att synkronisera räknarna istället byts ut mot ett steg att mellan enheterna utbyta, dvs. synkronisera, räknevärden före varje nyckelgenerering.

Enligt patentkraven uppräknas räknevärdet hos vardera enheten synkroniserat och periodiskt. Det anges inget i patentkraven om att uppräkningen skall ske vid vardera enheten oberoende av varandra, så som anges beträffande hur nyckeln genereras.

Såsom anförts av FMV tillhör det välkänd teknik inom krypteringsområdet att manuellt förse enheter som kommunicerar via en osäker kanal med nycklar i form av identiska uppsättningar numrerade nyckelblanketter, vilka skiftas samtidigt i fastställd ordning, exempelvis vid vissa tidpunkter eller efter varje meddelande. Enligt föreliggande uppfinning förses i stället enheterna med ett gemensamt utgångsvärde samt har var sin räknare, som räknas upp periodiskt och synkroniserat. Utgångsvärdet och räknevärdet utnyttjas som ingångsparametrar i en algoritm för att i vardera enheten oberoende av varandra generera en nyckel.

Av den teknik som anförts i målet får den i D3 visade tekniken anses vara den som kommer uppfinningen närmast. I D3 visas krypterad överföring mellan åtminstone två enheter i ett datakommunikationssystem via en osäker kommunikationskanal. I anslutning till en initieringsprocedur skapas ett gemensamt utgångsvärde (Kc) för användning i respektive enhet. I varje enhet finns en klocka vilken kan innefatta en räknare som periodiskt räknas upp. Klockornas synkronisering kontrolleras och till den ena klockans (slavens) värde adderas ett justervärde (offset) för att erhålla synkroniserade klockvärden. Vid vardera enheten genereras en nyckel utifrån utgångsvärdet samt räknevärdet resp. justerade räknevärdet och dessa nycklar används vid en efterföljande krypterad överföring.

Vad som anges i patentkravet 1 enligt förstahandsyrkandet skiljer sig således från vad som är känt genom D3 därigenom att det anges att ett räknevärde hos vardera enheten uppräknas synkroniserat och att dessa räknevärden används vid generering av en nyckel vid vardera enheten, medan i D3 ett uppräknat räknevärde används vid den ena enheten och ett justerat uppräknat räknevärde används vid den andra enheten vid generering av nycklar.

Det får dock i sammanhanget anses vara självklart för fackmannen att man i stället för att synkronisera två uppräknade räknevärden genom att till det ena addera ett justervärde välja att uppräkna de två räknevärdena synkroniserat. Detta särskilt mot bakgrund av att fackmannen inte kan uppfatta tekniken som beskrivs i D3 på annat sätt än att det ideala förhållandet är att de två räknarna (klockorna) uppräknas synkroniserat samt att vid förevarande uppfinning, trots att räknarna anges uppräknas synkroniserat, det framgår att behov av synkronisering kan föreligga.

För fackmannen som söker en alternativ metod till den som beskrivs i D3 framstår det därför som närliggande att välja att uppräkna räknevärdena synkroniserat i vardera enheten och på så sätt komma fram till en metod som anges i patentkravet 1.

Vid angivna förhållanden kan den i patentkrav 1 enligt förstahandsyrkandet angivna metoden inte anses skilja sig väsentligen från känd teknik.

Det självständiga patentkravet 8 enligt förstahandsyrkandet avseende ett datakommunikationssystem skiljer sig inte i fråga om det reella sakinnehållet från det självständiga metodkravets 1 innehåll på något avgörande sätt och anger därför inte heller en patenterbar uppfinning.

Vad gäller andrahandsyrkandets patentkrav 1 har i förhållande till förstahandsyrkandets patentkrav 1 införts bestämning om att ”enheterna efter en inledande synkronisering av räknarna endast utför kompletterande synkroniseringssteg vid behov”. Härvid konstaterar Patentbesvärsrätten att beskrivningen inte ger någon närmare upplysning om hur sådant behov fastställs eller villkor för att avgöra när sådant behov uppstått. En ytterlighet är då att behov anses föreligga kontinuerligt eller varje gång en nyckel skall skapas eller användas vilket synes motsvara patenthavarens uppfattning så som den kommer till uttryck i beskrivningen på s. 8, rad 11 - 17.

Vid den i D3 beskrivna tekniken kontrolleras klockornas synkronisering i slaven varje gång den mottar paket från mastern för uppdatering av justervärdet (offseten) och korrigering av detta vid förskjutning.

Vad som anges i andrahandsyrkandets patentkrav 1 skiljer sig således från vad som är känt genom D3, utöver skillnaden som diskuterats i samband med förstahandsyrkandets patentkrav 1, därigenom att räknarna synkroniseras, medan det vid tekniken enligt D3 sker en korrigering av justervärdet (offseten).

Det får dock i sammanhanget anses självklart för fackmannen att i stället för att addera ett justervärde i syfte att erhålla synkroniserade räknevärden välja att synkronisera räknarna.

Det framstår därför som närliggande för fackmannen som söker en alternativ metod till den i D3 beskrivna att förutom vad som

nämnts ovan om uppräknandet av räknevärdet även låta kompletterande synkroniseringssteg utföras endast vid behov och härvid komma fram till metoden enligt andrahandsyrkandets patentkrav 1, varför detta heller inte anger något patenterbart.

Då det självständiga patentkravet 7 enligt andrahandsyrkandet inte på något avgörande sätt skiljer sig i fråga om det reella sakinnehållet från det självständiga patentkravets 1 innehåll anger det därför inte heller någon patenterbar uppfinning.

De självständiga patentkraven som ligger till grund för patenthavarens yrkanden i tredje resp. fjärde hand motsvarar första- resp. andrahandsyrkandenas självständiga patentkrav, med den skillnaden att uttrycket ”kryptering och autentisiering” i de förstnämnda ersatt uttrycken ”kryptering eller autentisiering” resp. ”kryptering/autentisiering” i de sistnämnda. Denna bestämning får anses omfatta ett system eller en metod där samma nyckel används för både kryptering och autentisering.

Invändarna har anfört att det genom D7 och D9 är känt att vid kryptering och autentisering använda samma nyckel. Patenthavaren har inte bestritt att detta visas med dokumenten men har invänt att nyckeln inte genereras på samma sätt som vid uppfinningen. Vidare anges i D3 (s. 152) att syftet med separerade autentiserings- och krypteringsnycklar är att underlätta användningen av en kortare krypteringsnyckel utan att försvaga styrkan i autenticeringsproceduren.

Vid dessa förhållanden får det anses vara närliggande för fackmannen att vid något av första- eller andrahandsyrkandenas metoder eller system använda samma nyckel för kryptering som för autentisering, varför inget av sistahandsyrkandenas självständiga patentkrav anger något patenterbart.

Förutsättningar för att upprätthålla patent saknas sålunda varför patentet, med undanröjande av överklagade beslutet, skall upphävas.

Med denna utgång saknar Patentbesvärsrätten anledning att pröva huruvida uppfinningen skiljer sig väsentligen från vad som är känt genom övrig av invändarna anförd känd teknik samt att pröva frågan om huruvida beskrivningen av uppfinningen är så tydlig att en fackman med ledning av den kan utöva uppfinningen.

Per Carlson Stefan Svahn Sten-Ove Henningsson
Referent

ANVISNING FÖR ÖVERKLAGANDE, se bilaga 2 (Formulär A)