PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

BESLUT OM AVSLAG AV INVÄNDNING

Beslutsdatum **2003-12-12**

Patent nummer **0001044-7**

Adressat:

AWAPATENT AB

BOX 5117
200 71 MALMÖ SE

Patenthavare: **IMP International AB, Charlottenbergsvägen 4, 441 43 Alingsås SE.**

Ombud: **AWAPATENT AB.** Ref: **SE-2006358.**

Benämning: **Metod och system för kryptering och autentisiering.**

Brevet sänds till: **AWAPATENT AB, BOX 5117, 200 71 MALMÖ SE** och **FÖRSVARETS MATERIELVERK, PATENTENHETEN, 115 88 STOCKHOLM SE** och **DR LUDWIG BRANN PATENTBYRÅ AB, BOX 17192, 104 62 STOCKHOLM SE.**

Invändare I: **Försvarets materielverk.**
Ombud: **Försvarets materielverk, Patentenheten.**

Invändare II: **Telefonaktiebolaget LM Ericsson (publ).**
Ombud: **Dr Ludwig Brann Patentbyrå AB.**

B E S L U T

Er invändning mot ovan angivet patent har denna dag avslagits. Patentet är därmed fortfarande i kraft.

S K Ä L

Detta beslut avser kraven 1-13 i det beviljade patentet.

Uppfinningen avser en lösning för en krypterad överföring eller autentisiering mellan åtminstone två enheter via en osäker kommunikationskanal, och som är enkel och kostandseffektiv att implementera och använda, och dessutom erbjuder en hög grad av säkerhet. Detta åstadkoms bland annat genom en mycket begränsad överföring av data relaterat till säkerhetslösningen. Specifikt avser uppfinningen enligt patentet en lösning där ett räknevärde uppräknas synkroniserat och periodiskt i vardera enheten, helt självständigt och oberoende av den andra enheten. Utifrån denna samordnade uppräkning kan samma nycklar normalt genereras utifrån räknevärde och utgångsvärde samtidigt hos båda

Forts.

Ö V E R K L A G A N D E

Vill Ni överklaga beslutet skall Ni göra det skriftligt. Skrivelsen skall vara ställd till **Patentbesvärsrätten,** men sändas till *Patent- och registreringsverket, Box 5055, 102 42 Stockholm.* I skrivelsen skall anges det beslut som överklagas och den ändring i beslutet som begärs. Den skall ha kommit in till PRV inom två månader från beslutets dag. Ärendet kommer annars inte att prövas.

enheterna. Detta innebär att ingen inledande kommunikation normalt är nödvändig, vilket gör krypterings- eller autentisieringsprocessen både enklare och säkrare. I de ovanliga fall då synkroniseringen mellan enheterna av någon anledning brister kan synkroniseringssteget ske med stort tidsavstånd till den säkerhetsmässigt känsliga krypterings- eller autentisieringsprocessen, och dessutom behöver överföringen vid synkroniseringen endast ske i en riktning.

Fyra dokument har anförts i invändningsförfarandet, nämligen:
- D1: "Applied Cryptography", av B. Schneider, John Wiley & Sons, Inc., 1994
- D2: "Cipher Systems, The Protection of Communications" av H. Becker and F. Piper, Northwood Publications, 1982
- D3: "Specification of the Bluetooth System" Version 1.0 B, sidor 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), sidor 1-2,48-51.
- Även "notoriskt kända förfaranden vid substitutionschiffer, blankettchiffer, nyckelordschiffer och användningen av täcktabeller" har anförts.

D1 beskriver bland annat hur man genererar nycklar utifrån ANSI X9.17-standarden. Med hjälp av en basnyckel (k), ett startvärde (V) och ett (tids)räknevärde (T) genereras en slumpmässig nyckel R. Detta förfarande kan sägas överrensstämma med hur den slumpmässiga nyckeln genereras enligt uppfinningen. Dock föreligger en väsentlig skillnad, enligt uppfinningen genereras samma slumpmässiga nyckel synkroniserat och oberoende av andra enheter i minst en andra enhet. D1 löser inte problemet att synkroniserat och oberoende av den andra enheten generera en likadan nyckel i en första enhet. Genom detta förfarande behöver ingen okrypterad information utbytas mellan enheterna innan den egentliga informationen överförs via den osäkra kanalen. Tvärtemot beskriver D1 hur man överför redan genererade nycklar till andra enheter. Då D1 och uppfinningen inte berör samma problem och ingen hänvisning i D1 finns som skulle kunna leda fackmannen till en sådan slutsats är uppfinningen ny och uppfinningen anses även ej vara närliggande för fackmannen. Den enda gång okrypterad information behöver utbytas via den osäkra kanalen är om en synkronisering måste ske. Då synkroniserar enheterna sig så att dem använder samma räknevärde.

D2 beskriver en metod för hur nycklar skapas och används i ett system där information överförs mellan olika enheter. D2 beskriver hur man genererar nycklar för att användas för att kryptera information som ska sändas till en mottagare. En nyckel genereras utifrån ett utgångsvärde (base key) och en message key som ändras för varje nytt meddelande. I en vid tolkning kan man säga att message key kan liknas vid ett räknevärde som stegas upp för varje meddelande. Dock behöver inte message key vara en konsekutiv räkneföljdföljd, t.ex. ...7, 8, 9, 10... Sedan skickas message key till mottagaren tillsammans med det

Forts.

krypterade meddelandet. Det framgår tydligt på sidan 296 att message key måste skickas med till mottagaren. Dock finns en möjlighet för mottagaren att kunna räkna fram message key genom något som kallas "flywheeling". Genom att slumpmässigt generera den första nyckeln och sedan använda en "pseudo-random"-sekvensgenerator för att generera därpå följande nyckel kan mottagaren generera nästa message key om så skulle behövas. Behovet kan till exempel uppstå om kanalen som används är dålig och mottagaren missar den mottagna message key. Mottagaren kan då ligga i flywheeling under en kortare period tills synkronisering kan ske och därmed undvika att förlora meddelanden som sedan måste sändas om. Detta kan dock ej sägas motsvara uppfinningens idé att synkroniserat och oberoende av den andra enheten generera en likadan nyckel i en första enhet. Det D2 beskriver är ett system där message key ska skickas med varje meddelande och ett sätt att under en kortare period lyckas hålla kommunikationen uppe om kanalen skulle försämras och message key tappas. Däremot finns det inget i D2 som anses kunna leda fackmannen till en metod och ett system där en nyckel genereras i två enheter synkroniserat och oberoende av varandra så att ingen okrypterad information behöver skickas via den osäkra kanalen. Därmed är uppfinningen ny och uppfinningen anses även ej vara närliggande för fackmannen.

D3 är en specifikation av Bluetooth systemet. D1 beskriver att alla bluetooth-enheter, dvs. master och slav som etablerar en kommunikationslänk synkroniserar sina klockor. En del av masterklockans värde "clock" sänds till slaven under etablering av förbindelsen i så kallade FHS-paket. Detta värde tillsammans med kontinuerlig synkroniseringsbaserade accesskoder innebär att varje slav i förbindelse med en master är synkroniserad. Räknevärdet motsvarar alltså ett värde "clock" från masterklockan som räknas upp. Se sidan 160. Vidare beskriver D3 att en nyckel "payload key" genereras vid vardera enheten utifrån ett utgångsvärde Kc samt räknevärdet clock. Dessa nycklar används sedan för krypterad överföring eller autentisiering. Dock överförs synkroniseringsinformation kontinuerligt mellan enheterna som en del i varje meddelande. Därmed går också D3 tvärtemot uppfinningen att en nyckel genereras i två enheter synkroniserat och oberoende av varandra så att ingen okrypterad information behöver skickas via den osäkra kanalen. Vidare anses uppfinningen och D3 behandla olika områden. Bluetooth (D3) gäller för korta avstånd på några metrar i allmänhet och används för att enheter som en dator, trådlöst tangentbord eller trådlös mus ska kunna kommunicera med varandra och överföra information i realtid såsom musrörelser och tangenttryckningar. Uppfinningen hänför sig åt att kunna överföra krypterad information eller kunna utföra en autentiseringsprocedur över ett längre avstånd. Uppfinningen inriktar sig på att kunna överföra information (typ textmeddelanden). Även om denna distinktion inte direkt görs i uppfinningen och D3 så anses detta vara intuitivt. Fackmannen som vill lösa problemet att synkroniserat och oberoende av andra enheter generera likadana nycklar i två separata enheter för därefter autentisera eller överföra krypterad information skulle inte söka en sådan lösning i D3. Ej heller skulle fackmannen som tar del av D3 ledas till att konstruera ett system för överföring av information av typ textmeddelanden mellan två enheter på ett större avstånd. Därför anses D3 inte kunna utgöra ett hinder för patent.

Forts.

D4 beskriver kryptering och autentisiering inom GSM- systemet. Genom en initieringsprocedur genereras ett gemensamt utgångsvärde Kc. Denna används tillsammans med ett räknevärde (count) för att kryptera information som sedan sänds över en osäker kanal. Dock kan inte räknevärdet count sägas uppräknas oberoende i varje enhet då den beror på "TDMA frame number" Då denna information överförs via kanalen kan inte D4 sägas visa en metod eller ett system där en nyckel genereras i två enheter synkroniserat och oberoende av varandra så att ingen okrypterad information behöver skickas via den osäkra kanalen.

Vad gäller "notoriskt kända förfaranden vid substitut-ionschiffer, blankettchiffer, nyckelordschiffer och användningen av täcktabeller" som diskuterades på den muntliga förhandlingen 2003-11-26 så anfördes att även sådana system skulle kunna utgöra hinder för patentet. Genom att två enheter som önskar utbyta information bägge innehar en uppsättning nycklar som exempelvis kan vara numrerade 1, 2, 3, 4... När den ene användaren önskar överföra information till den andre överför denne i meddelandet först ett nyckelnummer med vilken den påföljande texten är krypterad, sedan skickas själva informationen. Mottagaren vet då vilken nyckel denne skall använda för att dekryptera informationen. Dock innebär detta system att nyckelnumret för överförs okrypterad samt att nyckelnumret alltid måste överföras vilket går tvärtemot uppfinningstanken. Dessutom genereras inga nycklar utan man använder på förhand genererade nycklar som har numrerats på något sätt för att kunna identifieras. Därmed anses inte "notoriskt kända förfaranden vid substitutionschiffer, blankettchiffer, nyckelordschiffer och användningen av täcktabeller" kunna utgöra några hinder för patent.

Eftersom samtliga dokument beskriver system där nycklar eller synkroniseringsinformation överförs kontinuerligt mellan olika enheter kan ingen sägas avslöja något som skulle kunna leda fackmannen till att konstruera ett system eller en metod där en nyckel genereras i två enheter synkroniserat och oberoende av varandra så att ingen okrypterad information behöver skickas via den osäkra kanalen. Därmed är uppfinningen ny och anses skilja sig väsentligt från tidigare känd teknik.

Genom att generera en nyckel i två enheter synkroniserat och oberoende av varandra så löses det tekniska problemet att inte behöva överföra okrypterad information via en osäker kanal. Därmed har också uppfinningen teknisk effekt.

Forts.

Därmed beslutas att patentet ska upprätthållas i dess nuvarande lydelse och invändningarna därmed avslås.

Rune Bengtsson

Stefan Hansson

OGU