Mål nr 09-130

PATENTBESVÄRSRÄTTENS DOM

meddelad i Stockholm den 20 april 2012

Klagande
SmartTrust AB

Ombud: Lisbeth Söderman, Borenius & Co Oy Ab
Tallbergsgatan 2 A, 00180 Helsingfors, Finland

SAKEN
Patent på "Förfarande och system för kontrollering av apparatidentitet"

ÖVERKLAGAT AVGÖRANDE
Patent- och registreringsverkets (PRV) beslut den 18 februari 2009 angående p.ans. nr 0402931-0, se bilaga 1

DOMSLUT

Patentbesvärsrätten avslår överklagandet

Postadress	Besöksadress	Telefon	Fax	Org.nr
Box 24160 104 51 Stockholm	Karlavägen 108	08-450 39 00	08-783 76 37	202100-3971

REDOGÖRELSE FÖR SAKEN OCH FRAMSTÄLLDA YRKANDEN

SmartTrust AB ansökte den 30 november 2004 om patent på ”System and method for device identity check”.

Uppfinningen

Patentansökans beskrivning innehåller bl.a. följande om uppfinningens bakgrund och ändamål.

> Uppfinningen avser ett förfarande och system för att kontrollera identiteten av apparater i ett apparathanteringssystem i ett mobilt telekommunikationsnätverk, varvid systemet innefattar apparater som skall hanteras, en apparathanteringsapplikation på serversidan, en apparathanteringsapplikation på klientsidan och databaser samt ett gränssnitt mellan nämnda apparathanteringsapplikationer.
>
> GSM är, tillsammans med andra teknologier, en del av en evolution av trådlös mobil telekommunikation. The Global System for Mobile Communication (GSM) är en standard för digital trådlös kommunikation med olika tjänster, såsom t.ex. taltelefoni. Abonnentidentitetsmodulen, The Subscriber Identity Module (SIM), i GSM-telefonerna konstruerades ursprungligen som ett säkert sätt att koppla individuella abonnenter till nätet men håller nuförtiden på att bli en standardiserad och säker applikationsplattform för GSM och nästa generationens nätverk.
>
> Mobilstationen (MS) är den enda utrustningen som GSM-användaren ser av hela systemet. I själva verket består den av två skilda entiteter. Den egentliga hårdvaran utgörs av mobilutrustningen, the Mobile Equipment (ME), vilken består av den fysikaliska utrustningen, såsom radiomottagaren, visningen och digitala signalprocessorer. Abonnentinformationen finns lagrad i abonnentidentitetsmodulen, Subscriber Identity Module (SIM), som implementeras som ett smartkort.
>
> Med hänvisning till terminologin som används i detta dokument ingår mobilutrustningen, the Mobile Equipment (ME), och abonnentidentitetsmodulen, the Subscriber Identity Module (SIM) i mobilstationen, The Mobile Station (MS).
>
> Mobilutrustningen identifieras unikt av den internationella mobilutrustningsidentiteten, the International Mobile Equipment Identity (IMEI), som är en unik kod som svarar mot en specifik GSM-terminal medan SIM-kortet i sin tur identifieras av kretskortidentiteten, the Integrated Circuit Card Identity (ICCID), vilken bestämmer kortets serienummer och vilket innehåller den internationella mobilabonnentidentiteten, the International Mobile Subscriber Identity (IMSI), som identifierar abonnenten, en hemlig nyckel för autenticering samt annan användarinformation. IMEI och IMSI eller MSISDN är oberoende och kan därmed erbjuda personlig rörlighet.
>
> The Mobile Station Integrated Service Digital Network Number, MSISDN, är det internationella standardtelefonnumret som används för att identifiera en given abonnent. Operatören har abonnemanget i en databas i nätverket, vilken databas visar motsvarigheten mellan IMSI och MSISDN. Genom att sätta in SIM-kortet i en

annan GSM-terminal kan användaren ta emot och ringa samtal från denna terminal samt ta emot andra abonnemangtjänster.

Avancerade mobila tjänster som till exempel webbläsning, multimediameddelanden, mobil e-post, och apparathantering, kan användas endast om en mobiltelefon konfigurerats på ett korrekt sätt. Dock vet många kunder inte hur deras apparat skall konfigureras. Operatörer måste försäkra sig om att apparatkonfigureringen är snabb och enkel för kunden. Denna hanteringsprocess av apparatinställningar och applikationer kallas apparathantering.

I en apparathanteringssession ingår t.ex. autenticering (användarverifiering), apparatinventering (en apparathanteringsapplikation läser vilka parametrar och applikationer som installerats i telefonen för framtida beslut, som till exempel uppdatering, tillsättning och borttagande av saker från installationerna), kontinuerligt ombesörjande (en apparathanteringsapplikation till exempel uppdaterar parametrar på telefonapparaten, skickar applikationer till apparaten, utför uppdateringar av mjuk- och hårdvara), apparatdiagnostik (finnande av fel), etc.

Ett enkelt sätt att förse (provisionera) en apparat med konfigureringsparametrar, som till exempel information om anslutning (apparatinställningar) är att skicka nya inställningar per radio (over the air). Efter att ha mottagit inställningarna för att konfigurera telefonen, sparar kunden inställningarna helt enkelt på telefonen och kan sedan använda tjänsterna. För operatören kan en förenkling av tillgången till avancerade tjänster betyda högre användningsgrad, nya inkomster, och minskade kundhjälpsutgifter.

Då en mobil terminal ansluter sig till nätverket, skickar den en signal till nätverket som innehåller både IMSI- och IMEI-information. De svenska patentansökningarna 0302626-7 och 0303210-9 presenterar förbättrade lösningar för introduktion av en ny terminal eller SIM till nätverket.

Som följd av den teknologiska utvecklingen håller nätverksanslutna och mobila/trådlösa apparater på att bli alltmer komplexa, och som en följd därav, håller anslutna apparater också på att bli alltmer svårhanterliga. Konsumenter och operatörer beöver därför ett verktyg för ett mera behändigt och effektivt hanterande av apparater.

Apparathantering (device management) är den allmänt använda termen för teknologi som tillåter tredje parter att utföra de svåra procedurerna för konfigurering av mobilapparater å användarnas vägnar. Det finns otaliga fall där apparathantering behövs, såsom till exempel vid anskaffningen av en ny apparat, för fjärrhantering av tjänster, nedladdning av mjukvara, byte och tillägg av tjänster samt upptäckt av tjänster och provisionering osv.

SyncML Device Management (SyncML DM) tillåter hantering av apparater och applikationer, förenklad konfigurering, uppdateringar och stödfunktioner. Sponsorerat och stött av ledande trådlösa företag accelererar SyncM-initiativet utvecklingen och marknadsframgången av SyncML DS och SyncML DM-teknologier.

SyncML Device Management Protocol (SyncML DM) är därmed en standard för kommunikation mellan apparater och serversystem för apparathantering. Standardiseringsorganet är OMA, Open Mobile Alliance. Apparaten som skall hanteras har utrustats med en SyncML-användaragent i apparaten (d.v.s. en terminal eller telefon) som talar SyncML DM-språket.

Apparathanteringsapplikationer används typiskt av leverantörer av mobila tjänster. De används för kundomsorg och för att öka inkomster genom effektiv hantering av mervärdestjänster. Exempel på fall i vilka de används är provisionering av tjänster och inställningar, apparatdiagnostik, statistik samt uppgradering av hård- och mjukvara.

Eftersom den mobila apparaten ofta består av två entiteter – Abonnentidentitetsmodulen (SIM, Subscriber Identity Module) och terminalutrustningen - är bägge entiterna, som bygger upp "apparaten" av intresse i en apparathanteringsomgivning. Bägge två av dessa entiteter måste vara föremål för apparathanteringsåtgärder. En mobil tjänsteleverantör, som önskar utföra apparathantering över t.ex. SyncML DM använder de fakto innehåll från både telefonen och SIM-kortet. Det betyder att både utrustnings- och abonnentinformation tas i beaktande.

Här kallas ett system, som avser både telefonen och SIM-kortet, för ett förenat apparathanteringssystem, Unified Device Management system (UDM).

För detta ändamål måste därmed apparathanteringsapplikationen vara medveten om viss information om apparaterna som skall hanteras. Apparathanteringsapplikationen måste vara informerad om apparatens identitet, adress eller telefonnummer, vilken information har mottagits på något sätt.

Vanligen har apparathanteringsapplikationen helt enkelt väntat tills en abonnent har beslutat att initiera en session och sedan utfört självhantering. Den svenska patentansökan 0401242-3 av sökanden presenterar förbättrade lösningar för apparatupptäckt.

I en abonnentbaserad apparathanteringsomgivning håller man reda på apparater som skall hanteras med hjälp av en abonnentidentitet, såsom t.ex. IMSI, MSISDN eller ICCID. En mobil tjänsteleverantör baserar allting, som t.ex. fakturering av abonnenten, på abonnentidentiteten. Vad gäller OTA-adressering, representeras en abonnentidentitet av en destinationsadress.

Från abonnentperspektiv är det ett abonnemang (d.v.s. destinationsadressen) som fungerar i en telefon (utrustning), och denna telefon kan bytas ut. I en abonnentcentrerad omgivning är det möjligt att apparathanteringsapplikationen inte vet den relevanta typen av telefon som används, och denna information borde därför inhämtas någonstans ifrån.

I en telefonbaserad apparathanteringsomgivning håller man reda på apparater som skall hanteras med hjälp av identiteten av den individuella telefonutrustningen. Detta verkar naturligt när man beaktar alla inställningar och applikationer som finns i en individuell telefon.

Från ett telefoncentrerat perspektiv är det telefonen som plötsligt inte längre kan nås när en användare beslutar att byta till ett annat abonnemang. En mycket sannolik situation är en användare med ett företags- och ett privat abonnemang, vilka möjligtvis till och med använder olika mobila tjänsteleverantörer.

Problem uppstår då abonnenten byter till en annan telefon eller ett annat abonnemang även om en apparat eller ett abonnemang kan ha varit känt vid försäljningspunkten av abonnemanget och/eller telefonen. Då kan apparathanteringsapplikationen bli kvar med en oriktig kombination av en telefonidentitet och abonnentidentitet, såsom t.ex. destinationsadressen eftersom en apparat består av två entiteter i en

enhetlig apparathanteringsomgivning Unified Device Management (UDM) environment och existerar i själva verket endast i realtid.

Detta faktum ålägger nämnda problem för både UDM- och DM-apparathanteringsapplikationer som hanterar endast telefonen och inte SIM-kortet. I en telefoncentrerad omgivning kan inte den mobila tjänsteleverantören säkert känna till destinationsadressen. Han kan endast veta vilken destinationsadressen var vid den senaste sessionen. Detta antyder att alla serverinitierade hanteringssessioner endast är framgångsrika av en slump.

SyncML DM-apparathanteringsapplikationen i sin tur kan inte få tillgång till en telefon utan riktig destinationsadress. SyncML DM-apparathanteringsapplikationerna kan dessutom inte utföra en granskning av UDM-apparatidentiteten eftersom den inte kan tala med SIM-filhanteringsprotokoll.

I en UDM-omgivning har apparatidentiteten på apparater en kombinerad identitet som består av både telefonidentifierare och abonnentidentifierare. Den kombinerade identiteten kallas i detta dokument UDM-identitet i det följande.

Om en slutanvändare möjligtvis har förändrat kombinationen sedan den senaste apparathanteringssessionen ägde rum, skulle UDM applikationen ha en oriktig UDM-apparatidentitet. Följaktligen kan den önskade telefonen inte nås via det abonnemanget. Den önskade abonnenten (abonnemanget) använder inte längre samma telefon.

En lösning för att uppdatera apparathanteringsapplikationen till den aktuella situationen är att utföra kontinuerlig apparatupptäckt i enlighet med nämnda svenska patentansökan 0401242-3 av sökanden, vilken presenterar förbättrade lösningar för apparatupptäckt.

En annan omständighet som bör tas i beaktande är att apparatidentiteten är dynamisk, med vilket man menar att en apparatidentitet i sjäva verket endast existerar i realtid. En apparatidentitet existerar endast i det mobila nätverket då en terminal används (är påslagen) av ett aktivt abonnemang. Då den är avslagen kan den inte nås per radio. Konceptuellt sett existerar den inte just då. Konceptuellt definieras den som avslagen, "offline". När apparaten sätts på igen och dess status ändras från "offline" (avslagen) till "online" (påslagen) är apparaten "online" i det mobila nätverket.

För att förstå detta koncept, tänk också på en situation där slutanvändaren byter om mellan två telefoner genom att därmed flytta abonnemanget fram och tillbaka. En sådan slutanvändare använder sig av ett abonnemang och två telefoner genom att alltså använda två olika apparater.

I en förenad apparathanteringsomgivning består en "apparat" av två entiteter som i själva verket endast existerar i realtid. Denna realitet förorsakar problem för apparathanteringsapplikationerna. En del av svårigheterna diskuteras nedan. Dessa kan indelas i två kategorier:

1. Problem med apparater, som är "offline" d.v.s. inte möjliga att nås per radio, OTA.
2. Problem med okänd status.
3. Problem i anslutning till att man inte vet när en apparat kommer att vara "online" nästa gång.

Det är ett problem för apparathanteringsapplikationer när mobila apparater inte kan

nås. De kan t.ex. försöka sända upprepade SMS-meddelanden till telefonnumret även om apparaten har ljudlös status genom att därmed orsaka stockningar i SMS-C-centralerna och i applikationstjänsterna alldeles i onödan. DM-applikationerna vet inte alls när de möjligtvis kunde få en chans att slutföra sina hanteringsuppgifter mot en otillgänglig apparat.

Huvudproblemet är förstås att apparaten inte kan hanteras. För att bemöta denna situation är apparathanteringsapplikationen angelägen att utföra apparathanteringsåtgärder mot apparaten så fort den är online igen.

Uppfinningens avsikt är att finna nya lösningar för problemet med förändrade UDM-apparatidentiteter.

PRV avslog ansökan den 18 februari 2009 med motiveringen att uppfinningen saknade uppfinningshöjd med hänsyn till känd teknik och hänvisade till följande dokument.

D1: US 6 400 939 B1,
D2: US 2003 0027 581 A1

Yrkanden

SmartTrust har i Patentbesvärsrätten vidhållit ansökan med två alternativa patentkravsuppsättningar ingivna den 19 april 2011. De nya kravsuppsättningarna betecknas Prioritet 1 resp. Prioritet 2 och är avsedda att prövas i nämnd ordning. De självständiga patentkraven 1 och 16 enligt förstahandsyrkandet, Prioritet 1, har följande lydelse.

1. Förfarande för att kontrollera identiteter på apparater i ett apparathanteringssystem i ett mobilt telekommunikationsnätverk, varvid systemet innefattar apparater som skall hanteras, en apparathanteringsapplikation på serversidan, en apparathanteringsapplikation på klientsidan, och en databas, samt ett gränssnitt mellan nämnda apparathanteringsapplikationer, varvid databasen, som är ansluten till gränssnittet, innehåller apparatidentiteter, som innefattar identifierare för utrustningsinformation och identifierare för abonnemanginformation samt statusinformation för att beskriva om apparater som skall hanteras är online eller offline,
k ä n n e t e c k n a t av följande steg i valfri ordning
a) initiering av en apparathanteringssession via nämnda gränssnitt,
b) nämnda apparathanteringsapplikation på klientsidan läser utrustningsinformation samt statusinformation,
c) nämnda apparathanteringsapplikation på klientsidan sänder den lästa utrustningsinformationen samt statusinformationen, till gränssnittet,
d) varvid gränssnittet hämtar nämnda information som finns i databasen från databasen och utför en jämförelse mellan den tidigare sparade informationen och den rapporterade informationen och sänder situationen om utrustningsinformationen och statusinformationen till apparathanteringsapplikationen på serversidan,

e) nämnda databas uppdateras med ny utrustningsinformation om, utgående från jämförelsen i steg d), den tidigare lagrade utrustningsinformationen ändrats, varvid en apparathanteringssession mellan klientsidan och serversidan påbörjas.

16. Apparathanteringssystem i ett mobilt telekommunikationsnätverk för att kontrollera identiteten på apparater som skall hanteras, varvid systemet innefattar en apparathanteringsapplikation på serversidan, en apparathanteringsapplikation på klientsidan och en databas, och ett gränssnitt mellan nämnda apparathanteringsapplikationer, k ä n n e t e c k n a t av att
a) komponenten på klientsidan är för att läsa utrustningsidentiteten samt statusinformation och för att sända den lästa utrustningsinformationen samt statusinformationen, till gränssnittet,
b) gränssnittet är för att granska identiteten på apparater från en databas på apparatidentiteter, och för att hämta nämnda information som finns i databasen och utföra en jämförelse mellan den tidigare sparade informationen och den rapporterade informationen och sända situationen om utrustningsinformationen och statusinformationen till apparathanteringsapplikationen på serversidan, och
c) databasen är ansluten till gränssnittet och innehåller apparatidentiteter, som innefattar identifierare för utrustningsinformation och identifierare för abonnemanginformation samt statusinformation för att beskriva om apparater som skall hanteras är online eller offline och spara statusinformation då förändringar äger rum.

De självständiga patentkraven 1 och 16 enligt andrahandsyrkandet, Prioritet 2, skiljer sig från motsvarande krav enligt Prioritet 1 därigenom att kraven har tillförts bestämningarna dels att apparater som skall hanteras är försedda ”med Subscriber Identity Module SIM-kort” dels att apparathanteringsapplikationen på klientsidan finns ”på SIM-kortet av apparaten”.

Grunder

SmartTrust har till grund för sin talan hållit fast vid att uppfinningen är ny och har uppfinningshöjd.

Utveckling av talan

Till utveckling av sin talan har SmartTrust i Patentbesvärsrätten i huvudsak anfört följande.

Nyhet/Uppfinningshöjd
Det poängteras att i krav 1 steg d) sker en notifiering/trigger/alert till apparathanteringsapplikationen. Detta steg d) värderas som det mest unika och viktiga med detta patent. Genom det begränsade skyddsomfånget är detta förtydligat. Det är i detta sammanhang som skillnaden på

applikationsnivå och nätverksnivå är viktig vilket tidigare har påpekats, men som inte alls berörts i motiveringarna för avslaget i avslagsbeslutet. Noder i GSM-nätet såsom EIR är alltså inget nyhetshinder mot vårt patent och inte heller hinder mot uppfinningshöjd av följande orsaker.

Viktigt i uppfinningen är alltså:

Att det är ett förfarande för att notifiera en apparathanteringsapplikation om en statusförändring (dvs online/offline-status) hos en apparat med hjälp av information genererad av en applikation på apparaten själv.

Att uppfinningen baseras på att apparaten själv innehåller applikationen som agerar som klient mot serverapplikationen/apparathanteringssystemet. "Klientsidan" i krav 1 b) avser alltså applikationen på apparaten själv. I avslagsbeslutet från PRV anförs flera där noder i GSM-nätet agerar klient (retrieves information from HLR).

Detta är beskrivet i ansökan på sidan 15-17 enligt i figur 2-4.

D1 (US 6 400 939)
I bägge lösningarna, alltså både i uppfinningen och i D1, checkas om den equipment information (utrustningsinformation) som meddelas till en check applikation för ett visst abonnemang finns i en databas som listar upp abonnenters apparater.

Följden av denna check är dock helt olika i uppfinningen och D1 och vår uppfinning och metoden i D1 går därför ut på helt olika saker. I uppfinningen startas en apparat management session mellan apparat och server men i D1 spärras apparaten från användning.

Dessutom implementeras vår uppfinning helt på applikationsnivån, GSM noder eller databaser i GSM, såsom EIR, eller någon GSM nod ingår inte i själva förfarandet.

I D1 fås både IMEI och IMSI (alltså utrustningsinformation) enligt kraven från "terminal equipment" (enligt paragraf 5, raderna 15-30) med hjälp av en location updating (man lyssnar på signaler i nätverket) eller

från "mobile station" eller alternativt är "IMSI redan känt" och då ber man endast om IMEI. I vår uppfinning fås IMEI via en applikation på SIM-kortet. Denna skillnad framgår tydligt både i de ursprungliga kraven och de nya.

I uppfinningen används en applikation på SIM-kortet. I D1 används utrustning som kan tjuvlyssna på signalleringstrafik för att upptäcka nya apparater såsom man gör i D1. Vid användning av en SIM- applikation behöver man inte göra ändringar i ett fungerande signaleringssystem i den mobila telekominfrastrukturen, vilket man gör endast av ytterst kommersiella orsaker. Vår metod är exakt och effektiv. En nätverksbaserad metod är mycket prestandakrävande i drift. En sådan innebär mycket dataprocessande "i onödan" eftersom absolut största delen av signaleringstrafiken i nätverket berör gamla välkända apparater.

Då patentkraven 1 och 16 skiljer sig tydligt från D1 (en applikation på klientsidan läser utrustningsinformationen och meddelar denna till servergränssnittet) och vår uppfinning löser ett helt annat problem än D1, såsom behandlades ovan, tror vi att D1 inte kan utgöra något patenteringshinder.

D2 (US2003 0027 581)
Detta patent löser visserligen samma problem som vår uppfinning, se t.ex. styckena [0010] och [0011], men läget är ändå liknande här som i D1, dvs. det kan verka som om D1 skulle göra liknande saker som i vår uppfinning, dvs. nätverket får info om att en IMSI har en ny IMEI och detta registreras i en databas men lösningen är nätverksbaserad och utförs inte på applikationsnivå.

I vår uppfinning fås IMEI via en applikation på klientsidan, fördelaktigt på SIM-kortet, vilket naturligtvis innebär att IMSI är känd på applikationsnivån och den fås inte från terminalen.

Vår uppfinning implementeras dessutom helt och hållet på applikationsnivån, GSM-noder eller databaser i GSM, såsom EIR, eller någon GSM-nod ingår inte. Både D1 och D2 presenterar helt nätverksbaserade lösningar.

Det står tydligt i stycket [0013] samt [0038] , [0043] , [0048] och [0060] att terminalen ger IMEI och IMSI via location update eller attach proceduren, vilket är nätverksbaserat. I t.ex. krav 10 av i D2 fås IMEI från nätverket.

Vår uppfinning implementeras alltså helt på applikationsnivån. IMEI fås i uppfinningen genom en applikation på SIM-kortet som aktivt hämtas av en applikation på SIM. Skillnaden är tekniskt sett mycket stor.

I stycket [0013] sägs vidare att den automatiska detekteringen utförs av en nätverksentitet. I stycket [0014] beskrivs en utföringsform där en detekteringsmodul kopplad till nätverket utför detekteringen.

Också databasen där jämförelsen av registrerade IMEI/IMSI-par utförs sker i uppfinningen annorlunda eftersom uppfinningen lagrar apparatidentiteter i en databas på applikationsnivån och är oberoende av nätverkselement såsom HLR (vilket används i krav 4 av D2) eller MSC (som i krav 5 av D2).

Våra krav 1 och 16 uttrycker tydligt att det finns en applikation på klientsidan som läser utrustningsinformationen (device entity) och sänder denna identitet till gränssnittet (interfacet). Det finns ingen applikation vare sig i D1 eller D2 och ännu mindre en sådan som läser denna information och aktivt sänder den till gränssnittet mellan applikationerna på klientsidan och serversidan, för i D1 och D2 lyssnar man på nätverkssignaler. Det finns inget sådant gränssnitt heller i D1 eller D2. Vi anser därför att vår uppfinning är tekniskt sett helt annorlunda uppbyggd och implementerad än D1 och D2. D1 och D2 ger inte heller de fördelar som vi presenterat i t.ex. stycket som finns på sidan 8 av vår ursprungliga ansökan, raderna 11 - 15.

DOMSKÄL

Den patentsökta uppfinningen avser ett förfarande och ett system för att kontrollera identiteter på apparater i ett apparathanteringssystem i ett mobilt telekommunikationsnätverk. Uppfinningen enligt patentkrav 1

innebär i korthet att systemet innefattar apparater som skall hanteras, apparathanteringsapplikationer på serversidan och på klientsidan, ett gränssnitt mellan nämnda applikationer samt en databas ”ansluten till gränssnittet”. En apparathanteringssession initieras via gränssnittet varvid applikationen på klientsidan läser utrustnings- och statusinformation och sänder denna ”till gränssnittet”, som jämför den mottagna informationen med tidigare i databasen lagrad information, samt sänder resultatet av jämförelsen till applikationen på serversidan. Databasen uppdateras med den nya informationen om denna är ändrad i förhållande till den lagrade varefter apparathanteringssessionen mellan klientsida och serversida påbörjas.

Båda de i målet anförda dokumenten D1 och D2 beskriver arrangemang som i mobila kommunikationsnät kontrollerar huruvida en abonnentapparat finns registrerad i en databas. När det gäller D1 syftar kontrollen till att ge nätoperatören möjlighet att bestämma vilka typer av apparater som abonnenterna får använda i nätet.

D2, som får anses visa den teknik som kommer uppfinningen närmast, avser i likhet med denna ett arrangemang för att kontrollera identiteter på apparater i ett apparathanteringssystem i ett mobilt telekommunikationsnät. En utföringsform av det kända arrangemanget (se avsnitt 0056) innefattar en server med en apparathanteringsapplikation som övervakar abonnemangs- och apparatidentiteter. Servern mottar, med utnyttjande av nätverkets signalsystem SS7, identitetspar, dvs. samhörande abonnemangs- och apparatidentiteter (t.ex. IMSI/IMEI), och jämför dessa med tidigare i en databas i servern lagrade identitetspar för de aktuella abonnemangen. Om ett mottaget par inte matchar tillhörande lagrat par inleder servern en apparathanteringssession. Att databasen vid behov uppdateras får anses självklart och framgår indirekt av avsnittet. Överföringen av utrustningsinformationen till serversidan kan, enligt vad som anges i avsnitten 0038 och 0039, ske från terminalen som svar på en förfrågan som initieras i en s.k. ”attach procedure”, och det får anses självklart att det kan ske i samband med den nämnda utföringsformen.

Vad som anges i det självständiga patentkravet 1 enligt förstahandsyrkandet skiljer sig från vad som är känt genom D2 därigenom att det

anges att en apparathanteringsapplikation även finns på klientsidan och där läser och överför utrustningsinformation jämte statusinformation till serversidan. Härigenom åstadkoms enligt SmartTrust att det patentsökta förfarandet utförs på applikationsnivå till skillnad mot förfarandet enligt D2 som är nätverksbaserat. Någon statusinformation berörs inte i D2 eftersom den aktuella utföringsformen förutsätter att apparaten är online. Vidare får det anses självklart att någon typ av gränssnitt förekommer mellan nätet och servern i arrangemanget som beskrivs i D2.

För fackmannen som, i syfte att undvika ett nätverksbaserat förfarande, söker ett alternativ till det förfarande för kontroll av identiteter som beskrivs i D2 framstår det som närliggande att för överföring av abonnent- och apparatinformation till serversidan använda en apparathanteringsapplikation även på klientsidan. Placering av applikationen på apparatens SIM-kort framstår därvid som ett uppenbart alternativ. Vad slutligen angår klientsidans status framgår denna indirekt av kommunikationen mellan klient- och serversida.

Vid angivna förhållanden kan det förfarande som anges i det självständiga patentkravet 1 enligt förstahandsyrkandet inte anses väsentligen skilja sig från känd teknik. Kravet anger därför inte en patenterbar uppfinning.

Det självständiga patentkravet 16 enligt förstahandsyrkandet avseende ett apparathanteringssystem skiljer sig inte på något avgörande sätt i fråga om det reella sakinnehållet från förfarandekravets 1 innehåll och anger därför inte heller en patenterbar uppfinning.

Vad sedan gäller andrahandsyrkandets självständiga patentkrav 1 och 16 skiljer sig dessa från motsvarande krav enligt förstahandsyrkandet enbart genom den införda uppgiften att apparathanteringsapplikationen på klientsidan placeras på apparatens SIM-kort. En sådan placering framstår emellertid, såsom angetts ovan, som ett uppenbart alternativ. Ej heller patentkraven 1 och 16 enligt andrahandsyrkandet anger därför en patenterbar uppfinning.

Vid angivna förhållanden och då vad SmartTrust i övrigt anfört i överklagandet inte föranleder annat kan överklagandet inte bifallas.

ANVISNING FÖR ÖVERKLAGANDE, se bilaga 2 (Formulär A)

I avgörandet har deltagit patenträttsrådet Stefan Svahn, ordförande, och f. patenträttsrådet Sten-Ove Henningsson, referent samt adjungerade ledamoten Jon Bergman. Enhälligt.