

*CVO Antwerpen Zuid*  
*Centrum voor Onderwijsbegeleiding Antwerpen Zuid*

*Module Datacommunicatie*

*Docent : Marc Rosseau*

*BLUETOOTH*

*ALAIN NARINX*

*Schooljaar 2005 - 2006*

## **1. Inleiding**

### **1.1 Geschiedenis**

Bluetooth is een open standaard voor draadloze verbindingen (1) tussen apparaten op korte afstand. Dankzij Bluetooth kunnen bijvoorbeeld adresgegevens tussen mobiele telefoons worden uitgewisseld, kan snel vanaf een PDA worden geprint, of kan een mobiele telefoon worden uitgerust met een draadloze headset. De techniek is ontwikkeld door de Zweedse mobilfoon-fabrikant Ericsson.

Voor Bluetooth werd ontwikkeld, was het enige alternatief voor koppeling van apparaten op korte afstand de eenvoudige koperdraad in al zijn vormen. Een headset was zo verbonden via een audiokabel met de mobilfoon-eenheid. Dit had niet alleen snellere slijtage als gevolg, maar de gebruiker had ook een merkbaar gebrek aan draagcomfort.

Verschillende fabrikanten merkten dit, maar er was er één die het voortouw nam: Ericsson. Dit verlangen om een betere oplossing te vinden was niet alleen gestimuleerd door de bovenstaande reden (het zoeken naar een draadloze verbinding tussen mobiele telefoons). Er was ook de lamentabele toestand waarin Ericsson zich in de vroege jaren '90 bevond. Het was toen leverancier van telefonie-, GSM- en netwerkapparatuur, en had een duw in de rug nodig.

Daarom zijn wetenschappers van Ericsson in 1994 begonnen met het zoeken naar een goedkope manier om via een radioverbinding communicatie tot stand te brengen tussen mobiele telefoons en andere apparaten. Men had zich in dit project ten doel gesteld om allerlei kabels tussen mobiele telefoons en computers, koptelefoons, desktopapparaten en dergelijke overbodig te maken.

### **1.2 Onderzoeksteam**

Het concept en de manier waarop Bluetooth communiceert is niet het werk van een onderzoeksteam, maar van één man: de Nederlandse doctor-ingenieur Jaap Haartsen (° 1963). Deze oud-student van de faculteit Elektrotechniek van de Universiteit van Delft, en huidig hoogleraar Mobile Radio Communicatiesystemen, is nauw betrokken geweest in de ontwikkeling van Bluetooth. Deze man was overigens niet aan zijn proefstuk toe: hij promoveerde in 1990 cum laude op het proefschrift 'Programmable SAW detection for on-chip, programmable RF filters' op dezelfde universiteit. Dit proefschrift bevat al enkele basisideeën van het toen nog niet bestaande Bluetooth-protocol. Momenteel geeft deze man deeltijds les, en werkt hij deeltijds aan het verfijnen van het Bluetooth-protocol (2).



Figuur 1

Naarmate het onderzoek vorderde, werd het de wetenschappers duidelijk dat de toepassingsmogelijkheden voor een dergelijke korte-afstandsradioverbinding legio waren. Omdat Ericsson enkel maar een mobilfoon-fabrikant was, werd besloten tot het oprichten van de 'Bluetooth Special Interest Group' oftewel Bluetooth SIG.

Het promoten van Bluetooth bleek al gauw zijn vruchten af te werpen toen fabrikanten als Palm, Ericsson, IBM, Intel, Lucent Technologies, Microsoft, Motorola, Nokia en Toshiba zich aansloten in 1998. Wat verder ook heeft geholpen aan het succes was het feit dat de Bluetooth-standaard is ontwikkeld als een rechten-vrije, niet-bedrijfseigen standaard.

De Bluetooth-specificatie heeft ondertussen al enkele versie nummers versleten, en is momenteel de huidige Bluetooth 2.0 specificatie. Deze versie is geïntroduceerd in 2004, met het doel om de zogenaamde 'EDR' oftewel Enhanced Data Rate optie toe te passen in Bluetooth-producten.

### 1.3 Naamgeving en symbool

De naam Bluetooth verwijst naar de Deense Viking-koning Harald Blåtand (Harold I in het Nederlands). Hij was koning van Denemarken en Noorwegen van 935 and 936 respectievelijk tot 940. Harold I heeft op het grondgebied van het huidige Denemarken, Zweden en Noorwegen vrede gesticht tussen een groot aantal strijdende stammenvolkeren, en het Christendom geïntroduceerd. Wat mogelijk ook deze naamgeving heeft beïnvloed is het feit dat de Bluetooth-technologie is uitgevonden in de Zweedse stad Skåne. Dit was vroeger ook één van de gebieden waar Harald I de orde heeft hersteld.



Figuur 2

Naar analogie van de vreedestichtende Deense koning wilde men dat de Bluetooth-technologie verschillende technologieën verenigde.



Volgens het officiële PR-verhaal voegt het Bluetooth-logo twee oude Noorse runen samen, en wel deze van de initialen van Harald Blåtand. Links is er de rune Haglaz, dat er enigszins uitziet als het "groter als" teken, en analoog is aan de moderne letter H. Rechts staat de rune Berkanan, die min of meer de vorm heeft van de moderne letter B, en hier ook analoog aan is (3).

Sommige mensen beweren dat dit niet helemaal waar is, en dat deze naamgeving een liberale interpretatie was van een bekende Zweedse novelle genaamd "De lange schepen" van Frans Gunnar Bengtsson. Dit boek was een bestseller in Zweden en was geïnspireerd door oude Viking-verhalen.

Figuur 3

Bovendien is dit logo een variatie op een oud logo van Beauknit Textiles, een divisie van een bekende Amerikaans textielbedrijf.

Oorspronkelijk was "Bluetooth" de werknaam van het project. Maar bij gebrek aan een betere naam is het ook de definitieve naam geworden bij de marktintroductie.

### 2. Bluetooth SIG

Het Bluetooth Special Interest Group bestaat sinds 1998 en houdt regelmatig vergaderingen om de standaard up-to-date te houden met nieuwe technologische ontwikkelingen.

De oorspronkelijke initiatiefnemers voor het vormen van het consortium waren Intel, IBM, Ericsson, Nokia and Toshiba. Later zijn Microsoft, 3Com and Lucent Technologies bij de groep van promotors gevoegd. Ondertussen heeft Lucent Technologies zijn lidmaatschap overgedragen aan de twee spin-off bedrijven Agere Systems en 3Com. Merkwaardig genoeg heeft Intel tijdens zijn lidmaatschap nooit gebruik gemaakt van het recht om een product te ontwikkelen.

Andere bedrijven vanuit uiteenlopende industrieën zoals Apple Computer, HP, Nissan, Pioneer en Sony hebben later lidmaatschap aangevraagd en zijn momenteel geassocieerde leden.

Tot enkele jaren geleden was de Bluetooth SIG een semi-professionele organisatie waarin individuele werknemers van de voorgenoemde organisaties zetelden. In de laatste jaren is er een verregaande professionalisering doorgevoerd en heeft de

Bluetooth SIG zijn hoofdkwartier opgesteld in de Amerikaanse stad Bellevue, in de staat Washington.

Momenteel wordt de leiding waargenomen door Dr. Michael Foley en een kleine groep van marketingmanagers, ingenieurs en organisatoren. Verder wordt de dagelijkse taken uitgevoerd door vertegenwoordigers uit de verschillende bedrijven die lid zijn van het consortium.

Op regelmatige basis worden er evenementen georganiseerd om de interoperabiliteit te testen tussen verschillende nieuwe en bestaande producten. Ook legt men procedures vast voor de ontwikkeling van Bluetooth-compatibele producten.

### **3. Klassen**

Bluetooth is ontwikkeld als een radiografische standaard, die tegen een laag stroomverbruik, met een kort bereik en met een goedkope zender/ontvanger microchip kan gebruikt worden.

De standaard laat verschillende apparaten communiceren wanneer ze in het bereik komen van elkaar, zolang er een onderlinge afstand is van maximum 100 meter.

Het bereik wordt bepaald door de klasse van de Bluetooth-verbinding. Momenteel zijn er drie klassen:

- Klasse 1 (100 milliwatt): apparaten met een bereik van 100 meter (328 voet). Voornamelijk USB Bluetooth-zenders en PCMCIA-kaarten worden met zulke sterke zenders uitgerust en zijn vrij gemakkelijk te verkrijgen.
- Klasse 2 (2,5 milliwatt): apparaten met een bereik van ca. 10 meter (33 voet). Dit is de meest populaire klasse, waarin men vooral mobiele telefoons, computermuizen, toetsenborden en printers vindt.
- Klasse 3 (1 milliwatt): apparaten met een bereik tussen 10 en 100 centimeter (3,9 duim tot 3.3 voet). Deze klasse wordt voornamelijk gebruikt door producten die uitgerust zijn met een chip die een zeer laag verbruik heeft, zoals hoofdtelefoons.



Figuur 4

De bovenstaande cijfers zijn officiële standaarden, maar in de praktijk kunnen er afwijkingen zijn tot bijna 5 à 10 meter (zoals bij klasse 2 soms het geval is). Vooral in omgevingen waarin (edel)metalen of steen aanwezig zijn kan het bereik zowel positief als negatief fluctueren.

### **4. Toepassingen van Bluetooth**

Volgende apparaten maken gebruik van Bluetooth:

- Laptops en desktops met ingebouwde Bluetooth-chips, waar vooral Apple Computer en IBM (nu Lenovo) early adopters zijn. Ingebouwde chips zijn eigenlijk nog niet volledig ingeburgerd, maar elke computergebruiker kan gemakkelijk een Bluetooth-zender kopen die verbonden kan worden via de USB-poorten.
- Computer-toebehoren zoals muizen, toetsenborden en printers worden meer en meer uitgerust met ingebouwde Bluetooth-chips. Fabrikanten zoals Logitech, Macally, Apple en Canon bieden naast hun gewone gamma een reeks Bluetooth-muizen aan die vooral voor de mobiele en/of zakelijke gebruiker bedoeld zijn.

- Bluetooth-enabled mobiele telefoons zijn momenteel zeer populair omwille van de koppeling met een headset, die voorheen verbonden was door middel van een hinderlijke draad. Bovendien kunnen deze mobiele telefoons ook verbonden worden met personal computers, PDA's en verschillende andere handhelds. Hiervoor wordt het OBEX-protocol gebruikt.
- Enkele MP3-spelers en digitale camera's gebruiken Bluetooth om bestanden van en naar computers te zenden.
- Nieuwe medische apparatuur van Amerikaanse fabrikanten zoals Advanced Medical Electronics Corp. wordt uitgerust met Bluetooth-zenders (4).
- Sommige GPS-ontvangers gebruiken Bluetooth om NMEA-data uit te wisselen. NMEA-data zijn gegevens die uitgewisseld worden tussen GPS-ontvangers en marine-radars.
- Car kits van A-klasse wagens zoals Volvo, BMW, Toyota worden standaard uitgerust met Bluetooth-zenders om de voorheen hinderlijke draadverbinding te vervangen door een draadloze verbinding.
- Verbindingsstukken tussen gehoorapparaten en mobiele telefoons worden nu ook aangeboden met Bluetooth-zenders. Medische fabrikanten zoals Starkey Laboratories bieden hiervoor kleine koppelingen die verbonden kunnen worden met een gehoorapparaat (5).



Figuur 5

## **5. Specificaties, versies en eigenschappen**

Zoals eerder gezegd is Bluetooth ontwikkeld door Ericsson, en is later op punt gesteld door de Bluetooth Special Interest Group. Bluetooth is nu een open standaard geworden die ook bekend staat als IEEE 802.15.1.

### **5.1 Bluetooth 1.0 en revisie B**

Versies 1.0 en 1.0b waren onderhevig aan verschillende communicatieproblemen en de verschillende deelnemende fabrikanten van de Bluetooth SIG hadden moeite om hun producten met elkaar te laten samenwerken.

Eén groot obstakel in deze versies was de verplichting om het Bluetooth Hardware Device Address (afgekort als BD\_ADDR) te verzenden bij het handshaking-proces. Dit maakt anonimiteit onmogelijk op niveau van protocol, en is een bezwaar als bedrijven zoals reclamebureaus Bluetooth-services wilt aanbieden die gebaseerd zijn op het anoniem aanbieden van reclameboodschappen via Bluetooth.

### **5.2 Bluetooth 1.1**

In versie 1.1 zijn verschillende fouten opgelost die in de 1.0b specificaties aanwezig waren. Ook is er ondersteuning toegevoegd voor niet-versleutelde Bluetooth-communicatiekanalen. Tenslotte is er nog de Received Signal Strength Indicator of RSSI toegevoegd. Dat is een indicator om te meten hoe sterk het Bluetooth-signaal werkelijk is. Ondersteuning voor deze indicator was al reeds een tijd ingebouwd in het Wireless LAN protocol en Bluetooth is hier vrij snel in gevolgd.

### **5.3 Bluetooth 1.2**

Deze versie is compatibel met versie 1.1 en heeft enkele grote verbeteringen toegevoegd aan het Bluetooth-protocol, namelijk de volgende:

- Adaptive Frequency-hopping spread spectrum, wat een technologie is om nog beter vaak gebruikte radiografische frequenties te vermijden. Zo zullen er wederzijds minder storingen optreden.
- Hogere transmissiesnelheden.
- Extended Synchronous Connections, dat een protocol is die de stemkwaliteit van audioverbindingen verbetert. Dit wordt gedaan door foute datapakketten opnieuw door te sturen.
- Host Controller Interface ondersteuning voor 3-wegs UART.
- Host Controller Interface toegang tot timer-informatie voor Bluetooth-applicaties.

## **5.4 Bluetooth 2.0**

Deze versie is compatibel met alle 1.0 versies van het Bluetooth-protocol. De grootste wijziging in deze versie is de introductie van Enhanced Data Rate, dat met een snelheid van 2,1 Megabits gegevens kan doorsturen. Dit heeft de volgende effecten:

- De verbindingssnelheid is 3 keer groter als voorheen, en kan in de meest gunstige omstandigheden zelfs 10 keer groter zijn.
- Een lagere energieverbruik omdat er minder transmissies plaatsvinden.
- Vereenvoudiging van verbindingen met meer dan 2 apparaten door een grotere bandbreedte.
- Verbeterde BER (Bit error rate) prestaties.

## **5.5 Toekomstige versies**

Er zijn nog geen concrete producten naar buiten gebracht door de Bluetooth SIG, maar de volgende versie zal zeer waarschijnlijk snellere en langere verbindingen toestaan.

De toegenomen bandbreedte en verbeterde snelheid kan mogelijk een bedreiging vormen voor WiFi-technologie, maar deze vrees is niet echt gegrond: ook WiFi-chips worden steeds goedkoper en zuiniger met energie.

Omdat de Bluetooth-technologie vooral populair is geworden door de draadloze headsets, en de WiFi-technologie populair is geworden vanwege de eenvoudige internettoegang, zou het kunnen dat de twee technologieën onafhankelijk van mekaar kunnen blijven werken met elk zijn eigen accenten.

Bovendien heeft de Bluetooth SIG in mei 2005 aangekondigd te werken met de fabrikanten van Ultra Wide Band-apparatuur (UWB). Eenvoudig gezegd is UWB is een overkoepelende standaard die apparaten in staat stelt om draadloos met elkaar te communiceren, waarbij zeer korte pulsen gebruikt worden die nauwelijks langer dan enkele nanoseconden duren. Hierdoor kan de bandbreedte zeer breed gebruikt worden. UWB is overigens fundamenteel anders als andere vormen van radiocommunicatie; in tegenstelling tot normale radiocommunicatie gebruikt UWB geen radiogolven.



Figuur 6

In het licht van een samenwerking tussen UWB en Bluetooth-technologieën word de toepassing in Voice over IP-apparaten zeer interessant: het zou bijvoorbeeld kunnen dat er tussen een draadloze telefoon en een computer die luistert

naar VoIP-verkeer een Bluetooth-verbinding kan gelegd worden met UWB. Ook worden draadloze VoIP muziek en video-applicaties mogelijk zonder te wisselen van verbinding. Verder zijn er ook nog plannen om draadloos toegang te geven tot verkoopautomaten en reclame aan te bieden via Bluetooth.

## **6. OBEX**

Voor men technisch uitweid over Bluetooth is het belangrijk om te weten dat de gegevensoverdracht in Bluetooth wordt verzorgd door het OBEX-protocol. Dit protocol is niet alleen een grote steun voor Bluetooth vanwege zijn vele mogelijkheden, maar is eveneens een bron van vele veiligheidsproblemen die later in deze bespreking aan bod komen.

Deze standaard is al ouder dan het Bluetooth-protocol zelf en werd voorheen gebruikt in de IrDA-standaard (6). OBEX is de afkorting van OBject EXchange, en is een communicatieprotocol dat de uitwisseling van binaire objecten tussen verschillende apparaten vergemakkelijkt. De OBEX-standaard wordt momenteel onderhouden en bijwerkt door de Infrared Data Association maar is ook aangenomen door de Bluetooth SIG.

Eén van de eerste populaire toepassingen van OBEX was in de Palm III PDA. Deze Personal Digital Assistent en velen van zijn opvolgers gebruiken OBEX om vCards, gegevens en zelfs toepassingen uit te wisselen.

OBEX is gelijkaardig in design en functie als HTTP, in die zin tenminste dat een client-apparaat een betrouwbaar transportprotocol gebruikt om te verbinden met een server, en dat de server dan antwoord geeft of objecten terugstuurd.

Waar OBEX echter fundamenteel van verschilt van HTTP, is in volgende opzichten:

- **Transport:** HTTP is normaal gelaagd bovenop een TCP/IP-poort, terwijl OBEX gewoonlijk is geïmplementeerd op een IrLAP/IrLMP/Tiny TP stack op een infrarood apparaat. Bij Bluetooth is dit op de Baseband/LinkManager/L2CAP/RFCOMM-stack.
- **Binaire verzendingen:** Terwijl HTTP zijn informatie in gewone tekstvorm verstuurd, dat leesbaar is door mensen, stuurt OBEX binaire hoofdingen door om informatie uit te wisselen over een aanvrag of object. Dit is gedaan omdat apparaten met beperkte bronnen binaire bestanden zeer snel kunnen decoderen.
- **Sessie-ondersteuning:** Een HTTP-transactie is altijd sessieloos. Een HTTP-client opent één verbinding, stuurt één aanvraag, ontvangt zijn antwoord en sluit de verbinding. Bij OBEX kan één verbinding veel gerelateerde aanvragen en bewerkingen uitvoeren. De meest recente toevoegingen aan het OBEX-protocol laten zelfs toe dat abrupt gesloten verbindingen opnieuw kunnen geopend worden met alle sessieinformatie intact.

Uiteindelijk is het belangrijk om te weten dat OBEX het fundament is voor vele hogere Bluetooth-profielen. Deze profielen komen verder in deze bespreking nog aan bod, maar hier is al een korte opsomming:

- Generic Object Exchange Profile
- Object Push Profile
- File Transfer Profile
- Synchronization Profile
- Basic Imaging Profile
- Basic Printing Profile

## **7. Gebruikersprofielen**

Om Bluetooth te kunnen gebruiken moet een apparaat op protocolniveau kunnen interpreteren welke rol oftewel profiel de verbinding gaat krijgen. Het profiel bepaalt de mogelijke applicaties. Zo is het bijvoorbeeld niet de bedoeling dat een bestandsoverdracht via OBEX plaatsvindt op een headset.

Er wordt een onderscheid gemaakt tussen profielen die momenteel op de markt gebracht zijn door de Bluetooth SIG, en diegene die nog in ontwerp-fase zijn.

### **7.1 Advanced Audio Distribution Profile (A2DP)**

Ook wel benoemd als het AV-profiel, wordt gebruikt om een stereo audiostreaming mogelijk te maken tussen muziekapparaten zoals een MP3-speler en een headset of autoradio. Dit profiel hangt af op GAVDP. Er is eveneens ondersteuning inbegrepen voor "low complexity subband codec" (SBC) en kan optioneel de volgende bestandsformaten ondersteunen: MPEG-1, MPEG-2, MPEG-4 AAC en ATRAC van Sony. De I-Phono Hi-Fi Sport Headphones van Bluetake zijn een voorbeeld van een product die dit profiel gebruikt.



Figuur 7

### **7.2 Audio/Video Remote Control Profile (AVRCP)**

Dit profiel is ontworpen om een standaard interface te vormen om TV's, HiFi-toestellen met één afstandsbediening te kunnen bedienen. Mogelijk kan het samen met het A2DP of VDP-profiel gebruikt worden. Verder heeft dit profiel de mogelijkheid om uitgebreid te worden met fabriekseigen toevoegingen. Voor deze toevoegingen zal men het Generic Media Control Profile (GMCP) gebruiken. Dit is een open standaard voor transport van gegevens die betrekking hebben met de gebruikte media.

### **7.3 Basic Imaging Profile (BIP)**

Het BIP-profiel wordt gebruikt om afbeeldingen te zenden tussen Bluetooth-apparaten. Ook biedt BIP de mogelijkheid om deze afbeeldingen te vergroten of verkleinen en om de afbeeldingen om te vormen tot een geschikt bestandsformaat dat gelezen kan worden door het gebruikte toestel.

Het BIP-profiel wordt doorgaans in kleinere stukken onderverdeeld:

- Image Push: laat toe om afbeeldingen te zenden vanaf een apparaat dat de gebruiker bedient.
- Image Pull: laat toe om afbeeldingen te doorbladeren in een apparaat dat binnen het Bluetooth-bereik ligt, en om deze afbeeldingen op te halen.
- Advanced Image Printing: laat toe om afbeeldingen te printen met geavanceerde opties die het DPOF formaat gebruiken. Digital Print Order Format (DPOF) is een formaat die de gebruiker van een digitale fotocamera toelaat om te bepalen welke afbeeldingen hij wenst te printen, samen met informatie over de aantal afdrucken en andere afbeeldingsinformatie. Gewoonlijk bestaat DPOF uit een serie tekstbestanden in een speciale map op een Flash-geheugenkaart. Het formaat is ontwikkeld door Canon, Kodak, Fuji, and Matsushita.
- Automatic Archive: laat toe om zonder interventie van een gebruiker alle nieuwe afbeeldingen van een apparaat af te halen en te bewaren. Zo zou een computer bijvoorbeeld alle nieuwe foto's van een digitaal fototoestel kunnen halen wanneer dit apparaat binnen het Bluetooth-bereik van deze computer ligt.
- Remote Camera: laat toe om een gebruiker op afstand een digitale camera te bedienen. De techniek van de automatische sluitertijd na een gegeven aantal seconden kan dus vervangen worden door een techniek waarbij de gebruiker kan

plaatsnemen in een fotocompositie en via een Bluetooth-verbinding de sluiters van het fototoestel kan activeren.

- Remote Display: laat toe om een gebruiker afbeeldingen te zenden naar andere apparaten. Zo kan een gebruiker bijvoorbeeld een presentatie geven door dia's te zenden naar een digitale projector via Bluetooth.

#### **7.4 Basic Printing Profile (BPP)**

Dit profiel laat apparaten toe om tekst, e-mails, vCards en andere items te zenden naar printers, gebaseerd op afdrুকopdrachten. Het verschilt van het HCRP-protocol in die zin dat er geen printer-specifieke besturingsbestanden nodig zijn. Dit maakt BPP meer geschikt voor zogenaamde "embedded devices" zoals mobiele telefoons, digitale camera's en andere apparaten die een gebruiker niet eenvoudig kan updaten met de nieuwste printer-besturingsbestanden.

#### **7.5 Common ISDN Access Profile (CIP)**

Dit profiel geeft onbeperkte toegang tot de services, gegevens en signalen die het ISDN-protocol aanbiedt.

#### **7.6 Cordless Telephony Profile (CTP)**

CTP is ontworpen om draadloze telefoonapparaten te laten samenwerken met Bluetooth. Er is vanuit de Bluetooth SIG een visie ontstaan, genaamd "3-in-1 phone" waarin dat mobiele telefoons in de toekomst een CTP-gateway kunnen gebruiken via Bluetooth. Dit laat de mobiele telefoon toe om enerzijds te verbinden met een gewone PSTN-telefoonlijn wanneer een gebruiker in zijn huis of kantoor is, en anderzijds te verbinden met het publieke GSM, CDMA of UMTS-netwerk te verbinden wanneer er geen Bluetooth-verbinding beschikbaar is.

#### **7.7 Dial-up Networking Profile (DUN)**

Dit profiel voorziet een standaard om toegang te hebben tot het Internet en andere dial-up diensten over Bluetooth. Het meest gewone scenario is dat een gebruiker toegang zoekt tot Internet vanuit een laptop door via Bluetooth draadloos met zijn mobiele telefoon te verbinden. Dit profiel is gebaseerd op het Serial Port Profile (SPP) dat een Bluetooth-apparaat toelaat van een RS232 (of gelijkaardige) seriële verbinding te emuleren. Onder andere de AT commandoserie (verduidelijkt in ETSI 07.07) en het PPP-protocol vormen onderdeel van zowel het SPP als DUN-profiel. Vanwege dit feit is het gemakkelijk om in bestaande Bluetooth-producten SPP om te vormen tot DUN.

#### **7.8 Fax Profile (FAX)**

De bedoeling van dit profiel is om een duidelijk gedefinieerde interface te voorzien tussen een mobiele telefoon of vaste telefoonlijn en een computer waarop fax-programma's zijn geïnstalleerd. Er is ondersteuning aanwezig voor de ITU T.31 en ITU T.32 AT commando's, maar niet voor data en gewoon telefoonverkeer.

#### **7.9 File Transfer Profile (FTP)**

Naar analogie met die andere naamgenoot "FTP" (dat staat voor File Transfer Protocol) zorgt File Transfer Profile voor toegang tot het bestandssysteem op een ander Bluetooth-apparaat binnen het bereik van het netwerk.

Dit houdt tevens in dat de gebruiker een lijst van mappen kan bekijken, kan bladeren in het bestandssysteem, bestanden kan ophalen, terugzetten en wissen.

Dit profiel gebruikt OBEX als transportprotocol en is gebaseerd op GOEP, dat eveneens een Bluetooth-profiel is.

## **7.10 General Audio/Video Distribution Profile (GAVDP)**

Dit profiel vormt de basis voor A2DP en VDP.

## **7.11 Generic Access Profile (GAP)**

Dit profiel vormt de basis voor alle andere Bluetooth-profielen.

## **7.12 Generic Object Exchange Profile (GOEP)**

Generic Object Exchange Profile is een manier om een serie protocollen te definiëren die gebruikt worden door applicaties die OBEX gebruiken.

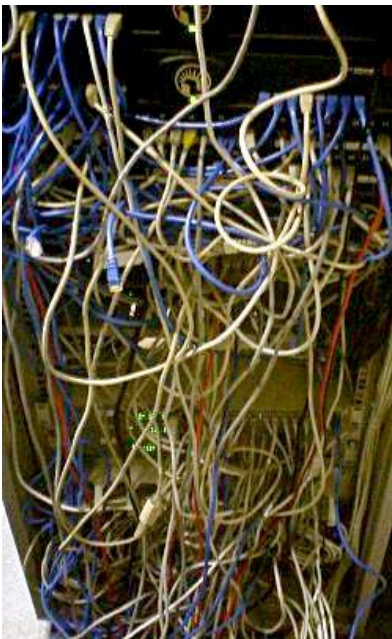
## **7.13 Hands Free Profile (HFP)**

HFP wordt gewoonlijk gebruikt voor handsfree car kits te laten communiceren met mobiele telefoons. Dit profiel gebruikt een eenvoudige versie van eSCO (extended Synchronous Connection Oriented), dat een manier is om een mono, PCM audiokanaal synchroon te zenden over een Bluetooth-verbinding.

Dit profiel wordt ook wel eens de "killer application" genoemd van Bluetooth: de applicatie die de invloed van Bluetooth zal verhogen. Dit komt omdat meer en meer landen het handenvrij telefoneren in de auto promoten, en aan elk persoon een zware boete oplegt wanneer men in de auto al rijdende belt met de mobiele telefoon in de hand.

## **7.14 Hard Copy Cable Replacement Profile (HCRP)**

Dit profiel biedt een eenvoudig alternatief aan de eeuwige kabelspaghetti die de kabels tussen computers, printers en andere randapparatuur vormen. Tot spijt van vele fabrikanten is er wel geen standaard gedefinieerd waarmee de eigenlijke communicatie tussen computer en printer plaatsvindt.



Figuur 8

Dit heeft als negatief gevolg dat dit profiel minder bruikbaar is voor "embedded devices" aangezien besturingsbestanden van printers niet zo eenvoudig zijn te laden op zulke apparaten.

## **7.15 Headset Profile (HSP)**

Zowat het meest gebruikte profiel voor headsets; levert ondersteuning voor deze populaire apparaatjes. Het gebruikt SCO voor de audioverbinding en een subset van de AT commando's van GSM 07.07 voor enkele eenvoudige commando's uit te voeren op de mobiele telefoon, zoals de mogelijkheid om een persoon op te bellen, een telefoonoproep te beantwoorden, te beëindigen of te weigeren, en om het volume te regelen.

## **7.16 Human Interface Device Profile (HID)**

Geeft ondersteuning aan apparaten zoals muizen, toetsenborden, joysticks en enkele alternatieve invoerapparaten. Het profiel is ontworpen om een verbinding te onderhouden met zeer weinig vertraging en een laag stroomverbruik, wat voor zulke invoerapparaten zeker zin heeft. Populaire apparaten die dit profiel gebruiken zijn onder andere de diNovo Media Desktop, een muis en toetsenbord-combinatie van Logitech en de Microsoft Optical Desktop Elite. In de toekomst zal de onuitgegeven PlayStation 3 spelcomputer ook Bluetooth HID ondersteunen zodat ook de entertainment-markt kan profiteren van deze technologie.

### **7.17 Intercom Profile (ICP)**

ICP wordt vaak vermeld als het "walkie-talkie"-profiel, en heeft in zekere zin ook zulke functionaliteit. Het profiel hangt af van SCO om de audiokanalen te zenden en ontvangen, en is ontworpen om eenvoudige telefoongesprekken te voeren tussen 2 Bluetooth handsets, zonder gebruik van het publiek telefoonnetwerk.

### **7.18 Object Push Profile (OPP)**

Een basisprofiel om "objecten" zoals afbeeldingen, vCards en vCalendars te zenden.

### **7.19 Personal Area Networking Profile (PAN)**

Het PAN-profiel laat toe om over Bluetooth verbindingen een zogenaamd Bluetooth Network Encapsulation Protocol te gebruiken. Dit protocol draait op de netwerklaag (laag 3) van het OSI-model, op een gelijkaardige manier als IPv6.

### **7.20 Serial Port Profile (SPP)**

Dit profiel is gebaseerd op de ETSI TS07.10 specificatie en gebruikt het RFCOMM-protocol. Het profiel emuleert een seriële kabel om een eenvoudige vervanging te bieden aan bestaande RS232-verbindingen mét draad. Het vormt de basis voor de DUN, FAX, HSP en LAN profielen.

### **7.21 Service Discovery Application Profile (SDAP)**

SDAP is aanwezig op elk toestel, en is een profiel dat verplicht moet gebruikt worden door de Bluetooth-zender om te ontdekken welke profielen aangeboden worden door de Bluetooth-ontvanger.

### **7.22 SIM Access Profile (SAP)**

Sim Access Profile laat toe dat apparaten zoals auto-telefoenen met ingebouwde GSM-ontvangers kunnen connecteren naar de SIM-kaart van een aparte mobiele telefoon. Op deze manier hoeft een auto-telefoon geen aparte SIM-kaart te gebruiken.

### **7.23 Synchronisation Profile (SYNCH)**

Het profiel zorgt ervoor dat PIM-items (Personal Information Manager) kunnen worden gesynchroniseerd. Omdat dit profiel oorspronkelijk deel uitmaakte van de IrDa infrarode specificaties, en later is aangenomen door de Bluetooth SIG, wordt dit profiel nog steeds vermeldt als "IrMC Synchronization".

### **7.24 Video Distribution Profile (VDP)**

VDP organiseert het transport van een video stream. Het zou bijvoorbeeld kunnen gebruikt worden voor streaming van een opgenomen video van een PC Media Center naar een draagbare speler, of van een digitale videocamera naar een televisietoestel.

Ondersteuning van de H.263 video-standaard is verplicht. Ondersteuning voor de MPEG-4 Visual Simple Profile, de H.263 profielen 3 en 8 zijn optioneel, en opgenomen in de specificatie.

### **7.25 Andere onafgewerkte profielen**

Er zijn nog enkele profielen die nog niet zijn afgewerkt door de Bluetooth SIG, maar wel zijn voorgesteld. Deze zijn de volgende:

- Handsfree Profile 1.5 (HFP 1.5)
- Unrestricted Digital Information (UDI)
- Wireless application Protocol over Bluetooth (WAP)

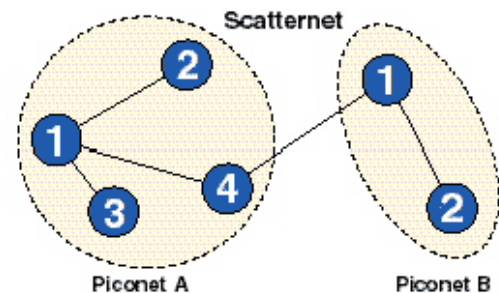
- Extended Service discovery profile (ESDP)
- Local Positioning Profile (LPP)
- Video Conferencing Profile (VCP)
- Device ID (DID): laat toe om een apparaat te identificeren aan de hand van de productversie, producent, programmaversie enzovoort. Het zorgt ervoor dat er applicaties kunnen toegepast worden die gelijkaardig zijn aan de Plug-and-Play specificatie.

## **8. Technische informatie**

### **8.1 Communicatie en connectie**

Eén Bluetooth apparaat speelt de rol van de "master" en kan communiceren tot en met 7 andere Bluetooth-apparaten die dan de rol van "slave" spelen. Zulk een netwerk van "7 slave + 1 master" Bluetooth-apparaten wordt piconet genoemd.

Op elk gegeven moment kan er tussen de master en 1 slave gegevens uitgewisseld worden. In zulk geval zal de rol van master en slave razendsnel omgewisseld worden om transport toe te laten.



Figuur 9

Gelijktijdige verzending van de master naar meerdere slaves is mogelijk, maar wordt in praktijk niet veel toegepast.

De Bluetooth-specificatie laat eveneens toe om 2 of meer piconetten samen te voegen. Wanneer dit plaatsvindt, wordt het netwerk een "scatternet" genoemd. In zo'n scatternet gedragen enkele apparaten zich als een brug tussen twee piconetten, door op het ene piconet de master-rol aan te nemen en in het andere piconet de slave-rol aan te nemen. Scatternetten worden in de praktijk tot nu toe nog weinig toegepast.

### **8.2 Initialiseren van een verbinding**

Elk Bluetooth-apparaat zal bij het initialiseren van een verbinding op aanvraag de volgende serie gegevens doorsturen:

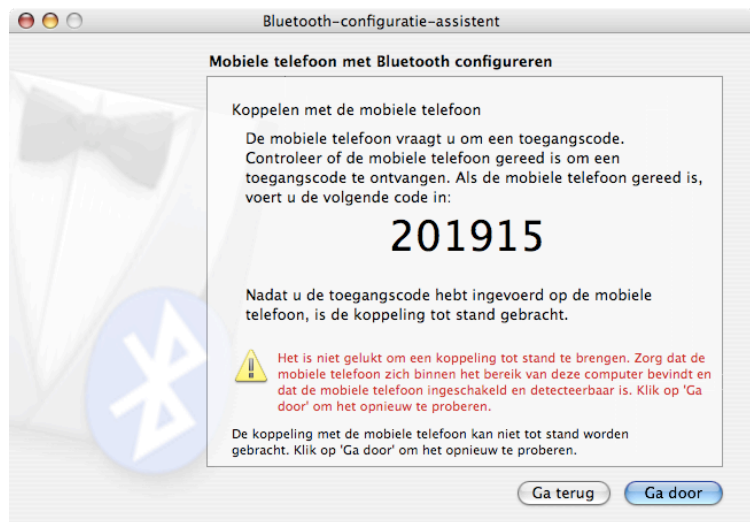
- Naam van het apparaat.
- Klasse van het apparaat.
- Lijst van aangeboden diensten (bv. telefonie, data en fax-verzending).
- Uitgebreide technische informatie (bv. eigenschappen, fabrikant en Bluetooth-versie van het apparaat, gebruikte profielen en aantal uren afwijking van GMT).

Elk apparaat kan een aanvraag doen om andere apparaten te vinden waar het naartoe kan verbinden, en elk apparaat kan ingesteld worden om te antwoorden op zulke aanvragen. Als het apparaat dat een verbinding probeert te initialiseren al gekend is bij het ontvangende apparaat, zal deze altijd directe verbindingsaanvragen positief beantwoorden, en alle informatie doorsturen die in de bovenstaande lijst vermeld staan.

Als één apparaat echter gebruik wilt maken van de diensten op een andere apparaat, zal er een "pairing" oftewel koppeling moeten plaatsvinden. Zo'n

koppeling wordt doorgaans beveiligd met een paswoord die vaak in de handleiding van een apparaat is te vinden. Over dit "pairing" wordt later nog meer uitgelegd.

Elk Bluetooth-apparaat heeft een uniek 48-bits netwerkadres, dat doorgaans verborgen wordt voor de gebruiker van het apparaat én voor de personen die met andere Bluetooth-apparaten het huidige apparaat ontdekken. In de plaats daarvan worden er wederzijds gebruiksvriendelijke "Bluetooth namen" getoond, die door de gebruiker zelf kunnen aangepast worden.



Figuur 10

Zulke gebruiksvriendelijke namen zijn meestal standaard ingesteld op de naam van het product of de netwerknaam van een computer. Soms kan dit wel eens verwarring opleveren wanneer men een koppeling probeert te maken met één apparaat wanneer enkele andere apparaten van het zelfde merk in het Bluetooth-bereik liggen.

Toch kan er voor diagnosedoeleinden het Bluetooth-netwerkadres opgezocht worden op de meeste apparaten. Op mobiele telefoons van Nokia kan dit bijvoorbeeld worden gedaan door de code "\*#2820#" in te tikken.

Op computers met Linux kan men het adres en klasse van een USB Bluetooth dongle vinden door het commando "hciconfig hci0 class" in te voeren als men met "root"-rechten is aangemeld. Mogelijk moet "hci0" vervangen worden door een andere apparaat-naam.

Het resultaat van dit commando is meestal het volgende:

```
BD Address: 00:10:60:A7:93:19 ACL MTU: 192:8 SCO MTU: 64:8
Class: 0x020005
Service Classes: Networking
Device Class: Miscellaneous
```

Uit bovenstaande gegevens kunnen we afleiden dat het Bluetooth-netwerkadres van de USB Bluetooth-dongle 00:10:60:A7:93:19 is, dat er een stereo audio-verbinding kan plaats vinden van 192 Kbps door 8 audiokanalen en een mono audio-verbinding van 64 Kbps door 8 audiokanalen.

Bovendien kan er uit bovenstaande gegevens ook afgeleid worden dat elk apparaat een 24-bits klasse-ID heeft. Deze ID levert informatie over welk apparaat dit is, en wordt ook verzonden wanneer andere Bluetooth-apparaten aanvragen doen op dit apparaat. Op een aantal mobiele telefoons en computers word deze klasse-ID vertaald in een symbool dat de klasse van het verbonden apparaat kenmerkt (bv. een icoon van een laptop, PDA of andere apparaten).

Bluetooth-apparaten zullen ook een lijst van diensten doorzenden wanneer er een aanvraag word gedaan door andere apparaten; dit houdt ook in dat er er extra informatie zoals de apparaatnaam, aangeboden diensten en kanalen worden doorgezonden. Deze kanalen zijn virtueel en hebben geen betrekking op de radiokanalen waarop ze worden uitgezonden via Bluetooth, maar zijn eerder analoog aan TCP-poorten. Een apparaat kan daarom probleemloos meerdere identieke services aanbieden. Onderstaande gegevens tonen dit aan.

```

Browsing 00:0E:ED:B0:AF:34 ...
  Service Name: OBEX Object Push
  Service RecHandle: 0x10000
  Service Class ID List:
  "OBEX Object Push" (0x1105)
  Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
  Channel: 9
  "OBEX" (0x0008)
  Language Base Attr List:
  code_ISO639: 0x454e
  encoding: 0x6a
  base_offset: 0x100
  Profile Descriptor List:
  "OBEX Object Push" (0x1105)
  Version: 0x0100

```

Technische gegevens voor het beheren van een verbinding kunnen eveneens opgevraagd worden van een Bluetooth-apparaat:

```

BD Address: 00:11:24:B3:50:FB
Device Name: Steves PowerBook
LMP Version: 2.0 (0x3) LMP Subversion: 0x7ad
Manufacturer: Cambridge Silicon Radio (10)
Features: 0xff 0xff 0x8f 0xfe 0x9b 0xf9 0x00 0x80
  <3-slot packets> <5-slot packets> <encryption> <slot offset>
  <timing accuracy> <role switch> <hold mode> <sniff mode>
  <park state> <RSSI> <channel quality> <SCO link> <HV2 packets>
  <HV3 packets> <A-law log> <CVSD> <paging scheme>
  <power control> <transparent SCO> <broadcast encrypt>
  <EDR ACL 2 Mbps> <EDR ACL 3 Mbps> <enhanced iscan>
  <interlaced iscan> <interlaced pscan> <inquiry with RSSI>
  <extended SCO> <EV4 packets> <EV5 packets> <AFH cap. slave>
  <AFH class. slave> <3-slot EDR ACL> <5-slot EDR ACL>
  <AFH cap. master> <AFH class. master> <EDR eSCO 2 Mbps>
  <EDR eSCO 3 Mbps> <3-slot EDR eSCO> <extended features>

```

### **8.3 Pairing in theorie**

Zoals eerder gezegd is een "pairing" oftewel koppeling van twee of meer Bluetooth-apparaten noodzakelijk wanneer deze apparaten van elkaars diensten gebruik willen maken.

Een koppel apparaten kunnen een vertrouwelijke relatie instellen door een gedeelde sleutelwaarde uit te wisselen, ook wel "passkey" genoemd. Een apparaat dat enkel wilt communiceren met een vertrouwd apparaat kan op cryptografische wijze de identiteit van het andere Bluetooth-apparaat valideren.

Apparaten die een vertrouwelijke relatie hebben ingesteld kunnen soms ook de verzonden gegevensstroom versleutelen zodat de gegevens niet kunnen afgeluisterd worden door derden. Deze versleuteling kan overigens uitgezet worden, en bovendien worden de passkeys bewaard op het bestandssysteem van het apparaat en niet de Bluetooth-chip zelf.

Aangezien het Bluetooth-adres van een apparaat onveranderlijk is, zal een koppeling altijd bewaard worden, ook al verandert één van de twee apparaten van naam. De koppelingen kunnen op elk apparaat eenvoudig verwijderd worden op elk gewenst moment als dit nodig is.

Sommige apparaten zoals Sony Ericsson mobiele telefoons zullen zelfs zonder pairing OBEX vCards en nota's accepteren. Enkele duurere merken van printers en Internet-toegangspunten laten Bluetooth-apparaten ook onbeveiligd gebruik maken van de diensten van het apparaat.

## **8.4 Pairing in praktijk**

De eerste stap in de pairing is bij elk apparaat hetzelfde: eerst wordt er bij beide toestellen een initialisatiesleutelwoord aangemaakt, en daarna een verbindingssleutelwoord, dat gebruikt wordt om de PIN-code te berekenen. Daarna worden deze sleutels uitgewisseld en vindt er validering plaats van de PIN-code. Als dat in orde is, dan moet een gebruiker de volgende stappen uitvoeren:

1. Bij mobiele telefoons, headsets, carkits en PDA's: Hier zijn er veel verschillende manieren van pairing, die op korte tijd niet kunnen uitgelegd worden. Wel bezit elk apparaat, uitgezonderd carkits en headsets, een commando om apparaten binnen het Bluetooth-bereik te vinden. Eens dat een apparaat is gevonden wordt een lijst getoond met de namen van de gevonden apparaten. Wanneer de gebruiker een apparaat selecteert voor koppeling, moet hij een PIN-code invoeren om zich te kunnen verbinden met het andere apparaat. Eens deze code is ingevoerd is er een koppeling en kan er uitwisseling van gegevens plaatsvinden.
2. Bij computers met Windows: Bij Microsoft Windows is de ondersteuning voor Bluetooth pas goed van start gekomen met de uitgave van Service Pack 2 van Windows XP. In deze uitgave zijn er standaard-drivers ingesloten die de meest bekende merken van Bluetooth-apparaten ondersteunen (Sony Ericsson, Trust, enz.).

Ondanks alle hulp is het installeren van Bluetooth-apparaten toch nog een karwei. De stappen die nodig zijn om dit succesvol te doen zijn de volgende (7):



Figuur 11

- a. Klik op Start, klik op Uitvoeren, typ "bthprops.cpl" en klik op OK.
- b. Klik in "Bluetooth-instellingen" op "Toevoegen".
- c. In de wizard "Bluetooth-apparaat toevoegen" schakelt u het selectievakje "Mijn apparaat is ingesteld en kan worden gevonden" in en klikt u op Volgende. Let op: U kunt niet op Volgende klikken voordat u het selectievakje Mijn apparaat is ingesteld en kan worden gevonden hebt ingeschakeld. Een apparaat waarvoor detectie is uitgeschakeld, kan tijdens een zoekopdracht niet worden gedetecteerd. Wanneer u op Volgende klikt, zoekt de computer naar detecteerbare apparaten die zich binnen bereik bevinden. Wanneer de zoekopdracht is voltooid, worden de apparaten weergegeven in de wizard.
- d. Selecteer het apparaat dat u wilt toevoegen en klik op Volgende.
- e. Wanneer u het gewenste apparaat hebt geselecteerd, kunt u een sleutel invoeren voor het apparaat. Een sleutel is een code die wordt gebruikt om de toegang tot een apparaat te beheren. Het gebruik van een sleutel helpt de beveiliging van de verbinding te verbeteren. Het is echter mogelijk dat er geen sleutel nodig is voor het apparaat dat u toevoegt. Wanneer u de sleutel invoert, probeert de computer verbinding te maken met het apparaat om de sleutel te controleren. Als u verbinding maakt met een andere computer, wordt een bericht weergegeven dat de computers verbinding proberen te maken.

f. Wanneer u de stappen op de computer hebt voltooid, voert u de sleutel in op het Bluetooth-apparaat. Als het apparaat een andere computer is, wordt op die computer een bericht weergegeven dat uw computer een verbinding aanvraagt. Voer deze stappen uit op de computer die u toevoegt als Bluetooth-apparaat:

- Klik in het bericht waarin staat dat uw computer een verbinding aanvraagt. De wizard Bluetooth-apparaat toevoegen wordt gestart en bevat een veld voor het invoeren van de sleutel.

- Voer de sleutel in. U kunt er ook voor kiezen om een sleutel te laten genereren. Wanneer de sleutel is gecontroleerd, is de verbinding voltooid. Het apparaat wordt nu weergegeven op de computer. Als het apparaat een andere computer is, wordt de computernaam weergegeven op de eerste computer.

- Op de laatste pagina van de wizard Bluetooth-apparaat toevoegen kunt u detectie uitschakelen op de computer die u als apparaat toevoegt. De optie om detectie uit te schakelen, is standaard geselecteerd zodat de computer niet voortdurend detecteerbaar is.

g. Nadat het apparaat is toegevoegd, wordt dit weergegeven in het onderdeel Bluetooth-apparaten. U kunt de apparaateigenschappen weergeven om de services te controleren, de naam van het apparaat te wijzigen of andere gegevens te verzamelen. U kunt ook verbindingen opzetten.

3. Bij computers met Mac OS X: Ondersteuning van Bluetooth in de Macintosh zelf en de ondersteuning van Bluetooth-apparaten is sinds medio 2002 aanwezig. Iets meer als 200 MB aan drivers voor zowel bekende als minder bekende fabrikanten zijn bij de standaardinstallatie bijgesloten.

Analoog met de bedrijfscultuur van Apple is de installatie van een Bluetooth-apparaat meestal zeer eenvoudig. Deze stappen zijn nodig:

a. Klik op het Bluetooth-icoon, rechts in de menubalk en selecteer "Configureer Bluetooth-apparaat".

b. Een wizard opent zich, waarbij de gebruiker selecteert welk apparaat hij wenst te koppelen, en hij op "Volgende" moet klikken.

c. Een lijst van gevonden Bluetooth-apparaten wordt gepresenteerd, en de gebruiker selecteert het apparaat uit de lijst en klikt op "Volgende".



Figuur 12

d. Het apparaat dat gekoppeld wordt zal om een nummer vragen, dat in grote letters op het beeldscherm van de computer staat. Na het invoeren van deze PIN-code is de koppeling voltooid.

## **8.5 Radioverbindingen**

Voor Bluetooth is een radiofrequentie uitgezocht die wereldwijd beschikbaar is. Het Bluetooth-protocol gebruikt de licentievrije ISM-band van het radiospectrum op 2,45 GHz. Dit had wat voeten in de aarde, want met name in Spanje, Japan en Frankrijk was deze radiofrequentie reeds in gebruik. Vooral in Frankrijk stelde de 2,45 GHz-band een probleem, omdat de Franse militaire machten deze frequentie actief gebruikten. Doorerschikking van de radiofrequenties heeft men daar

sinds 1 januari 2001 ook de 2,45 GHz-band voor Bluetooth ter beschikking kunnen stellen.

Juist vanwege het feit dat deze frequentie nu overal licentievrij is, wordt deze ook gebruikt voor babyfoons, afstandsbedieningen van garagedeuren, draadloze telefoons, magnetrons, en Wi-Fi-toepassingen. Om zo weinig mogelijk storing te veroorzaken met andere protocollen op de 2,45 GHz-band, verdeelt het Bluetooth-protocol deze band in 79 kanalen van elk 1 MHz breed en wisselt tot 1600 keer per seconde van kanaal.

Implementaties van Bluetooth versie 1.1 en 1.2 bereiken snelheden van 723 kilobits per seconde. Versie 2.0 neemt het Enhanced Data Rate (EDR) in gebruik en haalt hierbij snelheden van 2,1 megabits. Technisch gezien hebben apparaten met een Bluetooth 2.0-chip ook een hogere energieverbruik, maar omdat de gegevens 3 keer sneller dan voorheen kunnen gezonden worden, kan het verbruik van de chip effectief tot de helft van het gebruik dalen van Bluetooth 1.x-chips (veronderstellend dat men op alle chipversies dezelfde hoeveelheid gegevens zendt).

Alhoewel dat Bluetooth lijkt te concurreren met de WiFi-technologie verschillen de twee technologieën toch wel aanzienlijk. WiFi heeft een hoger gegevensdebiet, langer bereik maar heeft tevens duurdere en krachtigere hardware nodig.

Ze gebruiken dezelfde frequentieband, maar gebruiken verschillende multiplexing schema's. Terwijl Bluetooth een vervanging is voor allerlei soorten bestaande kabels, is WiFi enkel een vervanging van een netwerkkabel. Eenvoudig gezegd is Bluetooth een vorm van draadloze USB en is WiFi een vorm van draadloos Ethernet, waarbij beiden op een veel lagere snelheid werken als het bekabelde alternatief.

## **9.Beveiliging**

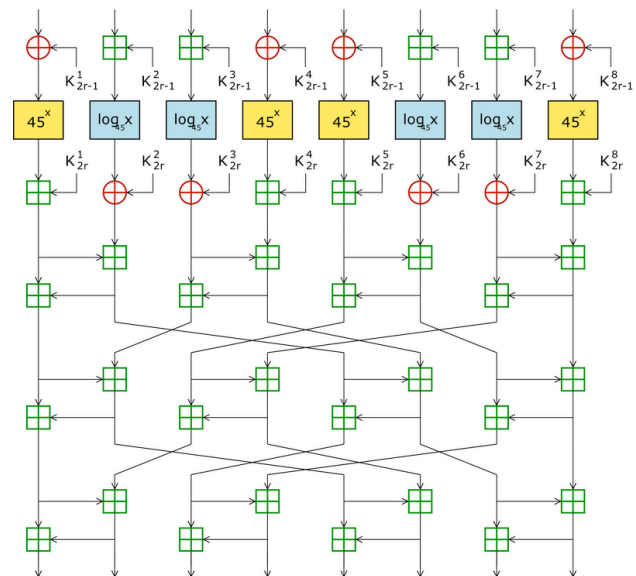
### **9.1 Beveiligingsmaatregelen**

Bluetooth gebruikt de SAFER+ algoritme voor het valideren van toegang en het aanmaken van gedeelde sleutelwoorden. Dit algoritme is in 1993 gepubliceerd door de Amerikaan John Massey.

Dit 128-bits licentievrije algoritme was eerst bedoeld om deel te worden van de bekende AES-standaard, maar uiteindelijk is dit niet gebeurd. Daarom heeft de Bluetooth SIG deze standaard aangenomen.

### **9.2 Gekende beveiligingslekken**

1. In november 2003 ontdekten Ben en Adam Laurie van het bedrijf A.L. Digital Ltd. dat er serieuze lekken zitten in het Bluetooth-protocol. Deze lekken konden leiden tot de onthulling van persoonlijke gegevens. De lekken zitten voornamelijk in het validerings- en gegevenstransport-protocol. Meer bepaald zijn er vier trends gevonden in de stroom van beveiligingsproblemen:



Figuur 13

- a. Vertrouwelijke gegevens kunnen anoniem worden verkregen, en zonder de toestemming van de eigenaar van het apparaat, vanuit sommige mobiele telefoons met Bluetooth. De betreffende gegevens zijn onder andere het volledige telefoonboek en kalender, en het IMEI-nummer van de mobiele telefoon.

- b. De volledige geheugeninhoud van enkele mobiele telefoons kan bereikt worden via een Bluetooth-apparaat dat voorheen op de lijst van gekoppelde apparaten stond (oftewel de "paired devices"), en daarna van de lijst is verwijderd. Het betreft hier wel degelijk alle gegevens van het bestandssysteem van een mobiele telefoon, dus ook mediabestanden als MP3's, opgenomen video's, foto's en SMS-berichten. Feitelijk kan een kwaadwillend persoon een volledige kopie maken van een Bluetooth-apparaat.
- c. Het is mogelijk om ook toegang te krijgen tot de zogenaamde AT-commandoserie. Daarmee kan een kwaadwillend persoon toegang krijgen tot de "hogere" niveau's van de mobiele telefoon zoals de telefonie-, fax- en data-diensten.
- d. De huidige "Bluejacking"-trend zet onwetende gebruikers ertoe aan om elk onbekend bericht met "ja" te beantwoorden, wat ertoe kan leiden dat een kwaadwillend persoon dit vertrouwelijke gebaar misbruikt om een virus in de mobiele telefoon te loodsen.

Deze problemen vloeien voort uit de volgende beveiligingslekken (8):

- a. Bluesnarfing: Het is mogelijk om te verbinden met een aantal Bluetooth-apparaten zonder de eigenaar van het apparaat te waarschuwen, en alle gegevens, ook de vertrouwelijke, te kopiëren. Gegevens zoals het volledige telefoonboek, de kalenders, de vCards, de ingestelde eigenschappen van het toestel, de "change log" en het IMEI-nummer kunnen gebruikt worden om de identiteit van een mobiele telefoon te klonen voor criminele doeleinden. Vanwege afspraken tussen Bluetooth-fabrikanten zijn over de lekken weinig details beschikbaar, maar de kwetsbaarheid zou zitten in het OBEX-protocol, dat door enkele fabrikanten foutief zou geïmplementeerd zijn.

Bluesnarfing is normaliter enkel mogelijk is als het Bluetooth-apparaat in "discoverable" of "visible" mode staat (respectievelijk ontdekbare en zichtbare modus). maar op sommige cracker-sites staan programma's om zelfs dit veiligheidssysteem te omzeilen.

- b. Backdoor-aanval: De backdoor-aanval houdt in dat het inbrekende apparaat een "pairing" heeft ondergaan met het slachtoffer, maar dat het inbrekende apparaat niet meer het register van gekoppelde apparaten staat. Op deze manier kan een kwaadwillend persoon zonder enige argwaan van het slachtoffer in zijn Bluetooth-apparaat inbreken, tenzij dat het slachtoffer juist het apparaat gebruikt als een connectie wordt gemaakt.

Na het onopgemerkt aanmaken van een Bluetooth-verbinding kan de kwaadwillende persoon gebruik maken van alle bronnen van het Bluetooth-apparaat. Het is niet alleen mogelijk om alle gegevens van het bestandssysteem op te halen (telefoonboek, afbeeldingen, enz.) maar het is ook mogelijk om het apparaat van het slachtoffer te misbruiken om toegang te verschaffen tot de GPRS, WAP of UMTS-diensten van het apparaat.

De enige manier waarop dat een slachtoffer kan merken dat het apparaat is aangevallen, is als het apparaat vroeger niet en nu wel kwetsbaar is voor bluesnarfing.

- c. Bluebug-aanval: Eerder in deze bespreking is het SPP-profiel ter sprake gekomen. Dit profiel bevat enkele lekken. Een bluebug-aanval gebruikt de Serial Port Profile om een serieel profiel-connectie aan te maken naar het apparaat. Op deze manier kan een kwaadwillend persoon volledige toegang krijgen tot de AT-commandoserie, die zoals eerder vermeld toegang geeft tot de "hogere" functies van een mobiele telefoon, zoals telefonie, fax- en datadiensten. Eens dat de toegang verzekerd is, kan er onder andere via het PPP-protocol voor gezorgd worden dat de internettoegang van een mobiele telefoon open staat voor misbruik. Maar het is tevens mogelijk om 0900-nummers te bellen, SMS-berichten te lezen en zenden, te verbinden met GPRS- en UMTS-diensten en zelfs conversaties in de buurt van de microfoon

van de mobiele telefoon af te luisteren. Deze laatste lek kan overigens gedaan worden via een gewone telefoonoproep over het GSM-netwerk, dus is het in theorie mogelijk om dit te gebruiken voor spionage op afstand.

Wat zo'n aanval nog gevaarlijker maakt, is dat terwijl een bluebug-aanval plaatsvindt, inkomende oproepen afgewezen kunnen worden. Dit stelt iemand in staat om inkomende oproepen af te leiden naar een zeer duur telefoonnummer, of naar een persoon die de identiteit van het slachtoffer aanneemt.

- d. Bluejacking: Dit fenomeen was al enige tijd bekend in de technische gemeenschap, maar is nu ook populair geworden bij doorsnee gebruikers van mobiele telefoons of laptops met Bluetooth.

Het probleem situeert zich in de zogenaamde "Bluetooth-naam", die ter vervanging wordt getoond van het Bluetooth-netwerkadres. Zoals eerder vermeld heeft elk Bluetooth-apparaat een uniek 48-bits netwerkadres, dat doorgaans verborgen wordt voor de gebruiker van het apparaat én voor de personen die met andere Bluetooth-apparaten het huidige apparaat ontdekken. In de plaats worden er wederzijds gebruiksvriendelijke "Bluetooth namen" getoond, die door de gebruiker zelf kunnen aangepast worden.

Bij het ontwikkelen van de specificatie voor deze Bluetooth-naam heeft men een zeer genereuze limiet gesteld van 248 karakters. Niet alleen is dit aantal karakters overdreven voor zelfs de meest veeleisende gebruikers, maar het is ook mogelijk om in zo'n grote naam een boodschap te zetten.

Zo is het bijvoorbeeld perfect haalbaar dat een kwaadwillend persoon met een laptop, die gevuld is met hacking-programma's, een Bluetooth-naam kan laten zien aan een nietsvermoedende mobiele telefoon-gebruiker in de stijl van "U heeft 10.000 euro gewonnen! Druk de pincode 7399 en bel naar 0900-666 666 om uw prijs te claimen!". In werkelijkheid zal het slachtoffer een koppeling accepteren, en de persoon met zijn laptop misbruik laten maken van zijn telefoon-diensten.

Feitelijk wordt het "raison-d'être" van Bluetooth-namen, het vereenvoudigen van het verbinden van apparaat naar apparaat, misbruikt om een boodschap toe te sturen. Deze boodschap kan een onwetend persoon ertoe aanzetten om een kwaadwillend persoon onbepaald toegang te geven tot de vertrouwelijke gegevens van zijn mobiele telefoon.

Doorgaans zullen de meeste mensen denken dat ze nooit zo dom zullen zijn om een bericht zoals de bovenstaande te accepteren. Overweeg dan toch het feit dat het fenomeen bluejacking bij doorsnee gebruikers soms wordt gebruikt als alternatief voor dating. Elk persoon is uiteraard gevoelig voor menselijk contact, en kan dus onder het voorwendsel van een leuke afspraak worden misleid om een Bluetooth-verbinding aan te maken met een kwaadwillend persoon.

Neem nu het scenario van een productmanager op zakenreis, die zijn smartphone gebruikt om zijn vliegtuigreis iets opwindender te maken dan de turbulentie voorziet. De productmanager zorgt ervoor dat zijn smartphone ontdekt kan worden door andere Bluetooth-apparaten, en toevallig zit er in het bereik van de man een kwaadwillend persoon met een laptop. Deze persoon met laptop heeft de bedoeling om bedrijfsgegevens te ontvreemden van nietsvermoedende gadgetdragende zakenlui, en door te verkopen aan de hoogste bidder. De productmanager ontdekt het Bluetooth-apparaat van de kwaadwillende persoon, die zich via de Bluetooth-naam voorstelt als een knappe blonde jongedame. De productmanager, misleid door dit aanlokkelijk aanbod, gaat in op dit aanbod in de veronderstelling dat hij een zeer interessant contact gaat leggen. In werkelijkheid is de bedrijfsspion met laptop de inhoud, contacten, afspraken en nota's van de zakenman aan het kopiëren waarin nieuwe productreleases staan.

Het voorbeeld hierboven toont aan dat er grote verliezen kunnen gepaard gaan met deze vorm van criminaliteit.

2. In april 2004 hebben beveiligingsconsultants van het bedrijf @Stake een beveiligingslek ontdekt waardoor het mogelijk is om lopende telefoongesprekken van een mobiele telefoon af te luisteren door via Bluetooth de PIN-code van een Bluetooth-headset te decoderen. Om dit probleem aan te tonen is er zelfs een concept-virus geschreven die gebruikt maakt van deze lek. Toch is er na uitvoerige demonstratie aan de fabrikanten van mobiele telefoons toch nog geen actie ondernomen tot nu toe.
3. In juni 2005 publiceerden Yaniv Shaked en Avishai Wool een paper genaamd "Cracking the Bluetooth PIN" (9), die laat zien hoe een kwaadwillend persoon zowel actieve als passieve methodes kan gebruiken voor de PIN-code te verkrijgen die nodig is om een Bluetooth-link aan te maken.

De passieve aanval zou toelaten dat een correct uitgeruste aanvaller een verbinding kan afluisteren en nadoen alsof de aanvaller deel uitmaakt van de koppeling tussen de twee afgeluisterde Bluetooth-apparaten.

De actieve aanval maakt gebruik van een speciaal gemaakt bericht dat op één bepaald punt in de initialisatie van het OBEX-protocol moet gevoegd worden. Dat zorgt ervoor dat de master en slave apparaten de "pairing" opnieuw initialiseren. Daarna moet het speciaal bericht opnieuw worden ingevoegd om de PIN-code te kraken. Het enige grote zwakke punt van deze aanval is dat de gebruiker zijn PIN-code opnieuw tijdens de aanval moet invoeren wanneer het apparaat erom vraagt. Bovendien is er nog een tweede, kleiner zwak punt en dat is dat bijna alle commerciële Bluetooth-apparaten niet capabel zijn om de juiste timing te leveren voor het speciaal gemaakt bericht op het juiste moment in te voegen.

4. Rond augustus 2005 heeft de politie van Cambridgeshire in het Verenigd Koninkrijk waarschuwingen uitgedeeld vanwege talloze auto-inbraken die met de hulp van Bluetooth zijn gepleegd.

De dieven gebruikten mobiele telefoons met Bluetooth om te detecteren of er in leegstaande auto's andere Bluetooth-apparaten zoals mobiele telefoons of laptops te vinden waren. Het bleek dat de meeste inbraken plaatsvonden bij automobilisten die hun mobiele telefoon met Bluetooth in zichtbare modus hadden laten liggen in de auto.

### **9.3 Voorkomen van beveiligingslekken**

Omdat Bluetooth een draadloze technologie is, heeft een gebruiker essentieel weinig tot geen controle over het bereik van de radiografische signalen. Het signaal kan eenvoudig opgepikt worden door kwaadwillende personen.

Daarom is het altijd belangrijk dat Bluetooth-gebruikers de aanbevelingen in de Bluetooth-standaard gebruiken, en proberen om zo weinig mogelijk koppelingen uit te voeren waarbij ze hun PIN-code moeten invoeren. Het is juist op het moment wanneer de PIN-code wordt doorgestuurd dat een Bluetooth-apparaat het grootste risico loopt om afgeluisterd te worden.

Sommige fabrikanten, voornamelijk die van de goedkopere apparaten, reageren op de beveiligingscrisis door een zogenaamd strikter beleid op hun apparaten in te stellen. Daarbij moet elke gebruiker de PIN-code op zijn Bluetooth-apparaat invoeren telkens als hij wenst te communiceren met een ander apparaat. Deze manier van werken geeft een vals gevoel van veiligheid, en stelt een gebruiker juist vaker bloot aan aanvallen op de PIN-code van zijn apparaat.

Ook zou het beter zijn dat fabrikanten van Bluetooth-apparaten de uitgewisselde PIN-code langer maken als 4 karakters. Momenteel gebruiken veel fabrikanten PIN-codes met de minimum lengte van 8 bits. Het is aangetoond dat zo'n code met een doorsnee Pentium 4-computer kan gekraakt worden in minder dan een kwart seconde.

Aangezien de Bluetooth-standaard toelaat om PIN-codes te verzenden met een lengte tussen 8 en 128 bits, zou het wisselijk zijn om het gemak van de klant even opzij te zetten voor meer veiligheid en een langer paswoord. Ook hier geldt het eeuwenoude mantra van de cryptografie: hoe langer het paswoord, hoe moeilijker de boodschap te ontcijferen is.

## **10.Concurrerende technologieën**

Bluetooth staat niet alleen in de markt met de draadvervangende technologieën. Omdat dit protocol in feite een vervanger is van standaard USB-verbindingen, ondervindt het heel wat concurrentie van zowel Europese als internationale standaarden, waarbij de ene standaard al wat efficiënter is als de andere.

De grootste bedreiging voor Bluetooth vormt Wireless USB, dat ook een vervanger is voor standaard USB-verbindingen. Hieronder een korte lijst van concurrenten:

- European Installation Bus: Open domotica-standaard, door het Belgische Konnex Association uit Diegem, die draadloze communicatie toelaat tussen controle-apparaten, computers, huishoudtoestellen en nutsvoorzieningen.
- HomePlug AV: Bedrijfseigen communicatie-protocol dat computers en entertainment-toestellen draadloos én via het stroomnet verbindt, voornamelijk gebruikt door fabrikanten van Home Cinema-toestellen.
- nanoNet: Een bedrijfseigen serie van draadloze sensorprotocollen, ontworpen om te concurreren met de ZigBee standaard, wordt voornamelijk gebruikt in industriële omgevingen en plaatsen waar controle op RFID-chips moet gebeuren.
- RadioRa: Bedrijfseigen tweewegs-protocol dat vooral gebruikt wordt om draadloos commando's te geven aan verlichting binnen en buitenshuis.
- TinyOS: Open-source besturingssysteem die de NesC-programmeertaal gebruikt om draadloos geïntegreerde sensors te laten communiceren, dat vooral gebruikt wordt door veel Amerikaanse universiteiten en enkele onderzoekers van Intel.
- Topdog: Een bedrijfseigen protocol voor draadloze netwerken, ontwikkeld door Watt Stopper en Legrand Inc. voor gebruik in de controle van residentiële en commerciële verlichting.
- UPB: Een nieuwe, zeer goedkoop te implementeren standaard voor tweewegs-communicatie over het stroomnet, waarbij verschillende apparaten en computers met elkaar kunnen communiceren. Ontworpen als opvolger en concurrent voor X10.
- WiFi: De gekende standaard voor WLAN-communicatie.
- Wireless USB: Open standaard, gebaseerd op ultra wideband draadloze technologie (zoals gedefinieerd in de onvolledige IEEE standaard 802.15.3a), die gebruik maakt van de bandbreedte tussen 3,1 tot 10,6 GHz in het radiospectrum. Onder andere HP, Microsoft, NEC Corp., Philips en Samsung maken producten met deze technologie, die een bandbreedte aanbied van 480 Mbits/s op 3 meter en 110 Mbits/s op 10 meter. WUSB gebruikt een ster-topologie die tot 127 apparaten kan ondersteunen, en waarbij toestellen een dubbele rol van slave en master kunnen aannemen (10).
- X10: Dit protocol voor communicatie over het stroomnet en over radiogolven is reeds in 1975 uitgevonden, en is voornamelijk gericht op domotica.
- Z-wave: Bedrijfseigen draadloos protocol voor controle van verlichting en het opvragen van de status van verschillende huishoudelijke apparaten.
- ZigBee: Een serie van protocols die voornamelijk dient voor de draadloze communicatie tussen gespecialiseerde radioapparatuur met een laag vermogen.

## **11. Inhoudsopgave**

Inleiding.....	2
Bluetooth SIG.....	3
Klassen.....	4
Toepassingen van Bluetooth.....	4
Specificaties, versies en eigenschappen.....	5
OBEX.....	7
Gebruikersprofielen.....	8
Technische informatie.....	12
Beveiliging.....	17
Concurrerende technologieën.....	21
Inhoudsopgave.....	22
Figurenlijst.....	23
Verklarende woordenlijst.....	24
Bibliografie.....	26

## **12.Figurenlijst**

Figuur 1: Pasfoto van Dr.Ir. Jaap Haartsen, de uitvinder van het Bluetooth-protocol.

Figuur 2: Standbeeld van koning Harald Blåtand, kan momenteel gevonden worden in de buurt van de Duitse havenstad Bremen.

Figuur 3: Het blauw-witte Bluetooth-logo.

Figuur 4: Een Bluetooth-headset van Motorola met een klasse 3 Bluetooth-chip.

Figuur 5: Een draagbare polysomnograaf van Advanced Medical Electronics Corp., die onder andere hartslag, EEG (registratie elektrische hersenimpulsen), EKG en andere gegevens kan registreren en via Bluetooth verzenden.

Figuur 6: Een draadloze VoIP-telefoonset van Motorola met ingebouwde Bluetooth en Ultra-Wide Band technologie.

Figuur 7: Een exemplaar van de I-Phono Hi-Fi Sport Headphones van Bluetake Inc. waarover in hoofdstuk 11.1 wordt gesproken.

Figuur 8: Kabelspaghetti, oftewel een wirwar van kabels, bij een router mét draden van een kleine onderneming.

Figuur 9: Typevoorbeeld van een piconet én een scatternet.

Figuur 10: De Bluetooth configuratie-assistent in Mac OS X die de gebruiker vraagt om een 6-cijferige PIN-code in te voeren op de mobiele telefoon.

Figuur 11: Een verzoek van de Bluetooth-wizard van Windows XP om de 4-cijferige PIN-code van een Bluetooth-headset van Sony Ericsson in te voeren in het invulveld.

Figuur 12: De Bluetooth configuratie-assistent in Mac OS X die de gebruiker een lijst van Bluetooth-apparaten aanbiedt die binnen het bereik van de computer liggen.

Figuur 13: Een klein deel van het wiskundig schema dat nodig is om het SAFER+ algoritme te berekenen.

### 13. Verklarende woordenlijst (chronologisch)

PDA: Personal Digital Assistant, oorspronkelijk de naam van de Apple Newton-toestellen, nu een algemene verzamelnaam voor alle elektronische handcomputers waarop informatie kan opgeslagen worden.

bedrijfseigen: Toestand van een concept of voorwerp waarin de licentierechten bij één commerciële onderneming rusten.

rune: Een letter of karakter uit het Oud-Noors, Scandinavisch geschrift dat rond 1000 na Christus is ontstaan.

spin-off bedrijven: Bedrijven die opgericht zijn rond een afgeleid product van een ander bedrijf, waarbij de opgerichte bedrijven dochterbedrijven zijn.

milliwatt: De watt is de SI-eenheid van vermogen. Eén watt staat gelijk aan één joule (eenheid van energie) per seconde.

Bluetooth-enabled: Een modewoord dat wordt gebruikt om aan te duiden dat een apparaat beschikt over een Bluetooth-microchip om draadloos te communiceren.

handheld: Zie PDA.

OBEX: OBject EXchange protocol, zie hoofdstuk 6 op bladzijde 7.

GPS: Global Positioning System is een draadloos systeem voor plaatsbepaling, waarbij satellieten in de atmosfeer van de Aarde door driehoeksmeting de plaats van een GPS-toestel kunnen bepalen.

car kit: Elektronisch systeem dat in auto's wordt ingebouwd, en dat via stemherkenning of controlehendels aan het stuurwiel ervoor zorgt dat een automobilist handenvrij kan telefoneren tijdens een autorit.

A-klasse wagens: Modewoord voor auto's met vele luxe-opties zoals klimatisatie, elektronische stuurcorrectie en dergelijke.

open standaard: Een industrie-standaard die kan worden aangepast door zowel particulieren als bedrijven, zolang de aanpassingen terug ter beschikking wordt gesteld van de gemeenschap.

specificaties: Bepalingen van een standaard of conventie.

UART: Een Universal Asynchronous Receiver Transmitter is een computerchip die parallele databits kan vertalen naar seriële databits.

BER: Bit error rate, oftewel foutentolerantie bij bits.

WiFi: Ook wel Wi-Fi technologie genaamd, zie hoofdstuk 10 op pagina 21.

Voice over IP: Ook wel VoIP genaamd, is de routing van telefonie-oproepen over IP-netwerken.

IrDA: Organisatie die de specificaties bepaalt van communicatieprotocollen die worden gebruikt op korte-afstand verbindingen, waarbij zenders en ontvangers communiceren met infrarood licht.

vCard: Een digitale business card.

HTTP: HyperText Transfer Protocol, een protocol om internetpagina's op te vragen en te ontvangen.

TCP/IP: Transmission Control Protocol/Internet Protocol, een set van communicatieprotocollen die de protocol stack op Internet implementeren.

headset: Modewoord voor een hoofdtelefoon, oftewel een luidspreker die direct in de gehoorgang kan geplaatst worden.

ISDN: Integrated Services Digital Network, origineel van het Duitse "Integriertes Sprach- und Datennetz", is een type van circuit geschakeld telefoonnetwerksysteem dat ontworpen is om digitale transmissie van telefonie en data toe te laten over standaard koperen telefoondraden, met een veel hogere snelheid en kwaliteit dan analoge systemen.

PSTN: Public Switched Telephone Network, oftewel de eerste en originele standaard voor telefonie die in de 19de eeuw zijn introductie maakte.

GSM: Global System for Mobile communications, de meestgebruikte digitale communicatie-standaard voor mobiele telefoons. Zeer populair in Europa, Azië, Rusland, Japan maar niet in de Verenigde Staten en bevriende staten als deze in de gebieden in de Stille Oceaan en het Midden-Oosten.

CDMA: Code Division Multiple Access, minder gebruikte communicatie-standaard voor analoge en digitale communicatie voor mobiele telefoons. Populair in de Verenigde Staten.

UMTS: Universal Mobile Telecommunications System, opvolger van het GSM-systeem.

dial-up diensten: Diensten waarbij er moet ingebeld worden op een centrale computer via het telefoonwerk.

HID: Human Interface Device, oftewel invoerapparaat.

GMT: Greenwich Mean Time, tijdstandaard op 0° oosterlengte. Greenwich ligt nabij Londen in het Verenigd Koninkrijk

pairing: Het koppelen van 2 elektronische apparaten via een Bluetooth-verbinding.

root-rechten: Beheerrechten op een computer.

dongle: Insteekmodule (doorgaans via USB-poort) voor een computer.

PIN: Afkorting van Personal Identification Number.

drivers: Besturingsbestanden voor een computersysteem.

wizard: Hulpprogramma bij populaire computerprogramma's om een ingewikkelde taak te vereenvoudigen aan de hand van vraagstelling aan de gebruiker.

debiet: Eenheid voor hoeveelheid doorgestroomd medium (water of gas bijvoorbeeld) per tijdseenheid.

embedded devices: Toestellen zoals PDA's, handheld computers en digitale foto- of filmcamera's die niet als primaire taak hebben om gegevens te verwerken.

IMEI: Uniek identificatienummer van een mobiele telefoon op een GSM-netwerk. Ingebouwd in de microchips van de mobiele telefoon zelf, niet in de SIM-kaart.

cracker: Persoon die inbreekt in computersystemen of computernetwerken voor eigen financieel gewin.

wireless: Engels synoniem voor "draadloos".

domotica: Samenvoegsel van "domus" (Latijns: huis) en "informatica", oftewel huisautomatisering.

## **14. Bibliografie**

- (1) David Parker et al. (2001) Wikipedia-artikel Bluetooth. Adres: <http://en.wikipedia.org/wiki/Bluetooth>. Wikimedia Foundation, St. Petersburg, Florida, Verenigde Staten van Amerika.
- (2) Ir. W.R. Van der Veen (2000) Dr. ir. Jaap Haartsen benoemd tot hoogleraar Mobiele Radio Communicatiesystemen. Adres: [http://www.utwente.nl/nieuws/pers/archief/2000/cont\\_00-072.doc/](http://www.utwente.nl/nieuws/pers/archief/2000/cont_00-072.doc/). Universiteit Twente, Twente, Nederland.
- (3) Pierre Abat et al. (2003) Wikipedia-artikel Koning Harold I. Adres: [http://en.wikipedia.org/wiki/Harold\\_I\\_of\\_Denmark](http://en.wikipedia.org/wiki/Harold_I_of_Denmark). Wikimedia Foundation, St. Petersburg, Florida, Verenigde Staten van Amerika.
- (4) Gary Havey (2005) Wearable Polysomnograph nieuwartikel. Adres: [http://www.ame-corp.com/Wearable\\_Polysomnograph.htm](http://www.ame-corp.com/Wearable_Polysomnograph.htm). Advanced Medical Electronics, Minneapolis, Verenigde Staten van Amerika.
- (5) Starkey Inc. (2005) Bluetooth in een hoortoestel. Adres: <http://www.starkey.nl/partner/content/view/20/2/>. Starkey Laboratories Inc., Eden Prairie, Minnesota, Verenigde Staten van Amerika.
- (6) Glade Diviney et al. (2005) Wikipedia-artikel OBEX. Adres: <http://en.wikipedia.org/wiki/OBEX>. Wikimedia Foundation, St. Petersburg, Florida, Verenigde Staten van Amerika.
- (7) Microsoft Corp. (2004) Knowledge base artikel 883259: Bluetooth-apparaten installeren en configureren in Windows XP Service Pack 2. Adres: <http://support.microsoft.com/kb/883259>. Microsoft Corporation, Redmond, Washington, Verenigde Staten van Amerika.
- (8) Adam Laurie & Ben Laurie (2003) Serious flaws in Bluetooth security lead to disclosure of personal data. Adres: <http://www.thebunker.net/security/bluetooth.htm>. A.L. Digital, Londen, Verenigd Koninkrijk.
- (9) Yaniv Shaked & Avishai Wool (2005) Cracking the Bluetooth PIN. Adres: <http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/index.html>. Universiteit Tel Aviv, Tel Aviv, Israël.
- (10) Khalid Hassani et al. (2005) Wikipedia-artikel Wireless USB. Adres: [http://en.wikipedia.org/wiki/Wireless\\_USB](http://en.wikipedia.org/wiki/Wireless_USB). Wikimedia Foundation, St. Petersburg, Florida, Verenigde Staten van Amerika.