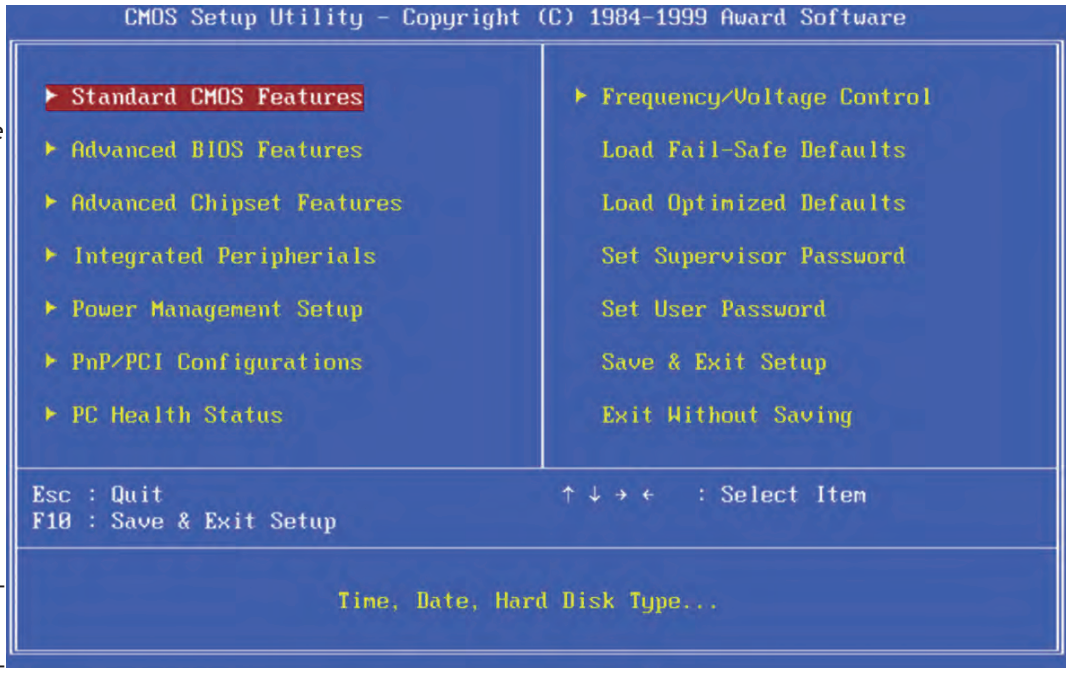
# UEFI, Secure boot en GPT

Hans Lunsing

De meeste nieuwe pc's hebben geen BIOS meer als vanouds, maar zijn uitgerust met zijn opvolger UEFI, ook wel UEFI-BIOS genaamd. UEFI staat voor 'Unified Extensible Firmware Interface' en is een software interface tussen het besturingssysteem van de computer en de firmware, de in zijn hardware geprogrammeerde software. UEFI zelf behoort natuurlijk ook tot de firmware van de computer. De huidige versie van UEFI is 2.4 van juli 2013.

## Inleiding

Veel UEFI-implementaties hebben een compatibiliteitsmodus waarin het oude BIOS wordt geëmuleerd door middel van de CSM (Compatibility Support Module). Vooral in eerdere implementaties was die modus ter wille van oudere software standaard geactiveerd. Maar ook als UEFI niet in de compatibiliteitsmodus werkt, zul je er als gebruiker in het algemeen weinig of niets van merken dat het oude BIOS is vervangen door een UEFI-BIOS.




*Instellingen voor de oude BIOS van Award uit 1999*

Dat verandert wanneer je bijvoorbeeld een ander besturingssysteem, zoals Linux, wilt installeren. Dit systeem en een daarbij benodigde bootloader (zoals Linux' Grub) zal met UEFI moeten kunnen werken, maar, belangrijker nog, Secure Boot zou wel eens roet in het eten kunnen gooien.

Sinds versie 2.2 van november 2010 maakt het door Microsoft voorgestelde Secure Boot-protocol deel uit van de UEFI-specificatie. Secure Boot beveiligt het opstartproces door te voorkomen dat besturingssystemen of drivers worden geladen die niet met een geldige digitale handtekening zijn ondertekend. Het zal geen verbazing wekken dat Microsoft de hoofdsleutel ('master key') voor de digitale handtekening beheert!

In 2011 veroorzaakte Microsoft nogal wat ophef door aan te kondigen dat computers alleen voor Windows 8 konden worden gecertificeerd als ze een UEFI-BIOS hadden, waarin Secure Boot met digitale handtekening van Microsoft was geactiveerd. Microsoft werd ervan beschuldigd het zo onmogelijk te maken dat alternatieve besturingssystemen, zoals Linux, konden worden geïnstalleerd.


*ROM BIOS firmware*

Microsoft ontkende dit echter door te stellen dat Secure Boot ook in een aangepaste modus moest kunnen werken of zelfs helemaal moest kunnen worden uitgeschakeld. Niet onlogisch, want er zijn ook Microsoftklanten die liever nog werken met een oudere versie van Windows (7 of Vista), die Secure Boot niet ondersteunt.
Voor we UEFI aan een nader onderzoek onderwerpen besteden we eerst de nodige aandacht aan het oude BIOS.

## Het oude BIOS

BIOS staat voor 'Basic Input/Output System'. Het is een basisvoorziening met een bibliotheek van instructies om het besturingssysteem met de hardware te laten communiceren. Bij het starten van een pc wordt het BIOS geactiveerd, dat eerst de Power-On Self Test (POST) uitvoert.
Tijdens de POST wordt gecontroleerd of de centrale processor (CPU), het geheugen (RAM), de videokaart, de opslagschijven, het toetsenbord en overige hardware normaal functioneren.

Als alles succesvol doorlopen is, zoekt het BIOS naar een opstartsector van een opslagschijf met een actieve partitie en zal het systeem verder worden opgestart op basis van de daarin gevonden informatie. De taak van het BIOS zit er dan op en wordt overgenomen door het besturingssysteem.

Het BIOS werkt nog steeds in 16-bit real mode. Besturingssystemen zijn inmiddels via 32-bit protected mode geëvolueerd naar 64-bit. Ze gebruiken de BIOS-interface dan ook niet meer, maar hebben hun eigen stuurprogramma's (drivers) voor randapparaten. De enige rol die nu nog voor het BIOS is weggelegd, is het geven van de aanzet voor het opstarten van het systeem.
De meeste BIOS'en bieden een ruime keuze aan instelmogelijkheden van de hardware, zoals CPU, geheugen, opslagmedia met volgorde van opstarten, video, audio, USB, LAN, etc. Ze zijn meestal toegankelijk door bij het opstarten een toets in te drukken. Welke toets dat is hangt af van het fabrikaat moederbord. Het is vaak een van de functietoetsen F2, F8 of F12 of de Del-toets.

De opstartsector van een harde schijf is 512 bytes groot en bevat het MBR (Master Boot Record). De eerste 446 bytes bevatten code voor het laden van een besturingssysteem, en bij modernere implementaties ook het tijdstempel en de signatuur van de schijf. De volgende 64 bytes bevatten de partitietabel met maximaal vier partities, terwijl de laatste twee bytes de boothandtekening bevatten.
Een van de vier partities kan worden 'uitgebreid', in die zin dat er maximaal 64 logische partities in kunnen worden geplaatst. Zo'n partitietabel wordt wel MBR of MSDOS-partitietabel genoemd.
Het BIOS dateert van 1981 en heeft sindsdien geen grote veranderingen meer ondergaan, zij het dat er wel aanpassingen zijn geweest om met nieuwere hardware, in het bijzonder grote harde schijven, te kunnen omgaan. Niettemin heeft het enkele belangrijke nadelen voor de steeds grotere systemen die het moest bedienen:
- 16-bit processor modus
- 1MB adresseerbaar geheugen
- per schijf is maar één bootloader mogelijk (in het MBR)
- maximum grootte op te starten harde schijf 2,2 TB
- ondersteunt alleen de x86-architec-tuur (pc AT-hardware), dus geen tablets en smartphones
- kan niet worden beveiligd tegen malware die bij het opstarten wordt geactiveerd.

UEFI is volledig nieuw opgezet om aan al deze nadelen een eind te maken.

## Het UEFI-BIOS

UEFI begon zijn leven in 1998 als een initiatief van Intel met de naam 'Intel Boot Initiative', later gepubliceerd als EFI. In 2005 ging EFI over in UEFI (Unified EFI), dat door vele IT-bedrijven, verenigd in het Unified EFI Forum, wordt gepropageerd en ondersteund.
Tot de deelnemende bedrijven behoren onder meer AMD, Apple, Dell, HP, IBM, Intel en Microsoft. De volledige specificatie van de opeenvolgende versies van UEFI is gepubliceerd op de website van het forum: http://www.uefi.org.

Unified Extensible Firmware Interface Forum

UEFI steekt in allerlei opzichten gunstig af bij het oude BIOS:
- ondersteuning voor 64-bit stuurprogramma's
- 17,2 miljard GB adresseerbaar geheugen
- ondersteunt meerdere bootloaders per schijf
- kan opstarten van zeer grote harde schijven (> 2,2 TB)
- (CPU) platform-onafhankelijk: draait o.m. op x86 (pc) en ARM (tablet)
- EFI heeft een shell voor het geven van opdrachten
- betere bescherming tegen rootkits en malware door Secure Boot
- sneller opstarten en ontwaken uit sluimerstand
- hardware interfaces, inclusief netwerk, worden al door UEFI ingeladen, zodat dit niet meer door het besturingssysteem hoeft te worden gedaan
- instellen is mogelijk via een grafische interface

UEFI kan met zowel 32-bit als 64-bit geheugenadressen zijn geïmplementeerd, maar moderne 64-bit systemen zullen uitsluitend 64-bit UEFI kennen. Een 64-bit UEFI kan alleen een 64-bit besturingssysteem starten.

*Grafisch scherm van GIGABYTE UEFI DualBIOS*

## Diensten van UEFI

EFI kent twee typen diensten: boot en runtime. De bootdiensten zijn vergelijkbaar met die welke het BIOS bood, maar omvatten ook tekst- en grafische consoles. Runtimediensten zijn ook nog beschikbaar wanneer het systeem al draait. De start- en verwerkingsinformatie voor al deze diensten is configureerbaar en wordt vastgelegd in een NVRAM (Non Volatile Random Access Memory) geheugen, waardoor de interface tussen het besturingssysteem en de firmware op het moederbord beter beschermd is.
Tot de runtimediensten behoren onder meer informatie over datum en tijd. Voor apparaten en andere onderdelen van de hardware kan voor elk besturingssysteem een standaard EFI-driver worden geschreven. Zo kan UEFI zelf de belangrijkste hardware interfaces (zoals USB, eSATA, audio) in het geheugen laden. Verder biedt UEFI twee grafische interfaces die niet afhankelijk zijn van specifieke VGA-hardware: het Graphics Output Protocol (GOP) en de Universal Graphics Adapter (UGA). MacOS X gebruikt GOP, terwijl Linux meest UGA gebruikt. Zo neemt UEFI alle communicatie met de hardware voor zijn rekening en vormt als het ware een minibesturingssysteem onder het eigenlijke besturingssysteem.

## De EFI-Shell

Een groot voordeel van EFI is de aanwezigheid van een shell. Deze shell kan worden gebruikt om UEFI-toepassingen, met inbegrip van UEFI-bootloaders, uit te voeren. Hij beschikt door middel van de UEFI-bootmanager over commando's voor:
- het opvragen van allerlei informatie over het systeem of de firmware, zoals de geheugenindeling (memmap)
- aanpassen configuratie van de bootmanager (bcfg)
- het draaien van partitioneringsprogramma's (diskpart)
- het laden van UEFI-drivers
- het bewerken van tekstbestanden (edit).

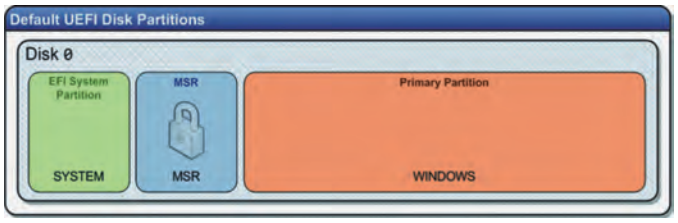
```
EFI Shell version 2.00 [4096.1]
Current running mode 1.1.2
Device mapping table
  fs0     :Removable HardDisk - Alias hd52g0b blk0
           Acpi(PNP0A03,0)/Pci(1D|7)/Usb(6,0)/HD(Part1,Sig90909090)
  blk0    :Removable HardDisk - Alias hd52g0b fs0
           Acpi(PNP0A03,0)/Pci(1D|7)/Usb(6,0)/HD(Part1,Sig90909090)
  blk1    :HardDisk - Alias (null)
           Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Primary,Master)/HD(Part1,Sig05BAE38B)
  blk2    :HardDisk - Alias (null)
           Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Primary,Master)/HD(Part2,Sig05BAE38B)
  blk3    :BlockDevice - Alias (null)
           Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Primary,Master)
  blk4    :BlockDevice - Alias (null)
           Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Secondary,Master)
  blk5    :Removable BlockDevice - Alias (null)
           Acpi(PNP0A03,0)/Pci(1D|7)/Usb(6,0)

Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Shell> _
```
*De EFI-shell*

Sommige implementaties van UEFI maken de shell beschikbaar via een optie in de firmware-instellingen, andere via het gebruik van een speciale toetscombinatie, en weer andere helemaal niet.
Sinds kort (Linux 3.3) is het mogelijk de Linuxkernel te configureren als een EFI-toepassing. UEFI kan Linux daardoor direct starten zonder dat er een opstartlader als Grub nodig is.

Een specificatie van de shell is te vinden op: http://www.uefi.org/specifications.

## De UEFI-Systeempartitie

EFI maakt gebruik van een extra partitie: de EFI System Partition (ESP). Deze bevat de bootloaderprogramma's voor alle geïnstalleerde besturingssystemen, drivers voor alle apparaten die door de firmware tijdens het booten worden gebruikt, systeemutilities die gedraaid worden voordat een besturingssysteem is gestart, en gegevensbestanden zoals foutenlogs. De EFI-partitie dient als FAT32 (FAT12 of FAT16 op verwisselbare media) te zijn geformatteerd en moet de eerste niet-verborgen partitie zijn. Zijn bootflag moet aan staan. Hij is gebruikelijk 100 tot 250 MB groot.




*Standaard UEFI-schijfpartities (volgens Microsoft)*

Bootloaders worden opgeslagen in leverancierspecifieke subdirectory's van de /EFI-directory.
Het UEFI-forum houdt een lijst van deze subdirectory's bij op http://www.uefi.org/registry. Een default bootloader kan worden opgeslagen in de directory /EFI/BOOT.

## Compatibility Support Module

Dankzij de Compatibility Support Module (CSM) kan UEFI, indien gewenst, op de oude BIOS-manier opstarten. Alleen dan wordt de code in het Master Boot Record (MBR) uitgevoerd. Bovendien kan CSM vaak selectief in- of uitgeschakeld worden voor specifieke apparaten.
In de eerste jaren van de toepassing van UEFI, in consumenten-pc's vanaf 2006, werd standaard de CSM ingeschakeld, soms zelfs zonder mogelijkheid naar UEFI om te schakelen. Er waren in die tijd immers nog geen besturingssystemen die met UEFI konden omgaan.
Veel pc's geven de mogelijkheid om, óf in UEFI óf via de CSM, in de oude BIOS-modus te starten. Sommige bieden deze keus zelfs direct in het opstartmenu, zodat je van gemengde modus ('mixed mode') kunt spreken. In dat geval kan het mogelijk en nodig zijn voor elk van beide modi een eigen opstartschijf in te stellen. In de toekomst zal de CSM in nieuwe UEFI-systemen niet meer beschikbaar zijn.

## De nieuwe GUID Partitietabel

Bij het UEFI-BIOS hoort ook een nieuwe indeling van harde schijven, in het bijzonder die waarvan het systeem opstart. Deze nieuwe indeling is vastgelegd in de GUID Partition Table (GPT) en is nodig om van zeer grote harde schijven (> 2,2 TB) te kunnen opstarten. GUID staat voor Globally Unique IDentifier, een pseudo-willekeurig getal van 16 bytes (128 bits) dat in softwaretoepassingen als identificatie wordt gebruikt en verondersteld wordt uniek te zijn.
Voordelen van de GPT ten opzichte van het oude MSDOS-schema zijn:

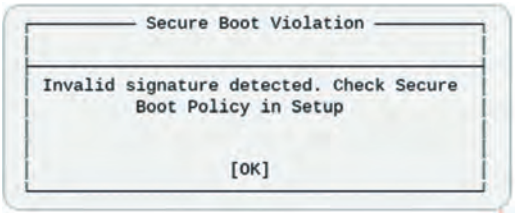
- Hij heeft unieke identificatienummers (GUID) voor schijven en partities
- Er zijn 128 partities mogelijk, terwijl dat bij het MSDOS-schema maar vier primaire, of drie primaire plus 64 logische partities zijn
- GPT kan zeer grote harde schijven aan, tot 9,4 ZB (dat is circa 9,4 biljoen GB), meer dan wat er nu op aarde aan opslagruimte is!
- GPT berekent een CRC32 (32-bits Cyclic Redundancy Check) om z'n integriteit te kunnen verifiëren
- Er wordt een back-up van de partitietabel bijgehouden
- GPT biedt betere bescherming tegen rootkits e.d., die zich in de opstartsector nestelen.

Elke schijf heeft één GUID, terwijl partities er twee hebben: één voor het type partitie en één voor een unieke identificatie van de partitie.
Een lijst van GUID's voor de verschillende partitietypes is te vinden op Wikipedia: http://tinyurl.com/parttypeGUIDs.

De eerste 32 sectoren (16384 bytes) van een schijf bevatten de partitietabel, terwijl aan het eind van de schijf een kopie is opgeslagen als back-up. De GPT-specificatie voorziet in een speciale BIOS-bootpartitie zonder bestandssysteem waarin bootloaders extra code kunnen plaatsen.
In het MSDOS-partitieschema werd daarvoor als gebruikelijk de 'DOS Compatibility Region' gebruikt, die bestaat uit ongebruikte ruimte tussen de bootsector en het begin van de eerste partitie.
De eerste sector van de EFI-systeempartitie bevat opstartcode voor compatibiliteit met BIOS-systemen. UEFI kan daardoor ook nog overweg met het oude MSDOS-partitieschema met een MBR. Sommige implementaties van UEFI doen dat echter niet rechtstreeks, maar via de CSM (Compatibility Support Module). In dat laatste geval wordt de bootsector (MBR) geraadpleegd, net zoals het oude BIOS doet.
Oudere programma's voor het bewerken van partities kunnen niet met GPT overweg. Om GPT daartegen te beschermen heeft een GPT-schijf een zogenoemde PMBR (Protective MBR, ofwel beschermende Master Boot Record). Dit toont de software een onbekende partitie die de hele schijf omvat. Bovendien kan de PMBR een bootloader bevatten om een oude BIOS (of de CSM!) in staat te stellen een GPT-schijf te booten. Voorwaarde daarvoor is natuurlijk wel dat die bootloader GPT begrijpt. Een voorbeeld van zo'n bootloader is Grub2, de bootloader van de meeste Linuxdistributies.

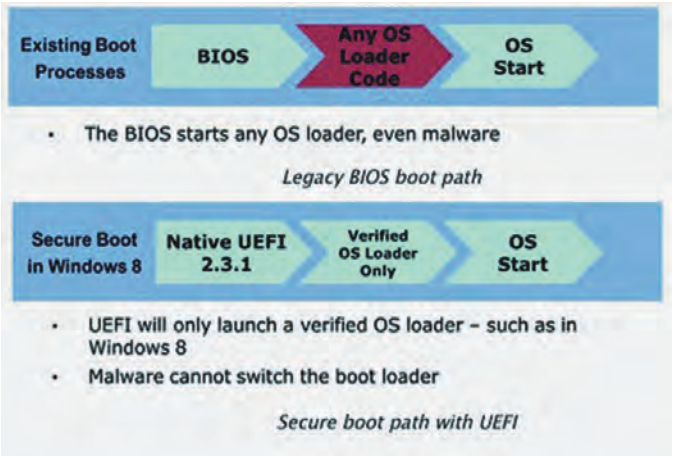
## Secure Boot

Secure Boot is pas in november 2010 met versie 2.2 aan de UEFI toegevoegd. Het protocol beveiligt het opstartproces door te verhinderen dat drivers of besturingssystemen worden geladen die niet met een geldige digitale handtekening zijn ondertekend.




Wanneer Secure Boot werkzaam wordt gemaakt, wordt het protocol aanvankelijk in instellingsmodus ('set-up mode') gezet, zodat een openbare sleutel met de naam Platform Key (PK) naar de firmware kan worden geschreven. Normaliter wordt dat door de fabrikant gedaan, maar Secure Boot kan ook in set-upmode worden afgeleverd.
Zo gauw de PK in de firmware is opgenomen, komt Secure Boot in de standaardmodus ('standard mode') waarin alleen nog software die met dezelfde sleutel is ondertekend zal worden toegelaten. Secure Boot kan echter ook in aangepas-

te modus ('custom mode') worden gezet, waarin extra openbare sleutels voor andere platforms (besturingssystemen) aan het systeem kunnen worden toegevoegd. Daarbij is het de bedoeling dat juist de uitgevende partij van het besturingssysteem de sleutel tekent om de herkomst te garanderen. In beginsel zou ook de gebruiker sleutels kunnen toevoegen als hij de software vertrouwt.
Op gewone pc's, laptops en notebooks (Intel- en AMD-systemen) kan Secure Boot door de gebruiker worden uitgeschakeld om een besturingssysteem te kunnen installeren dat Secure Boot niet ondersteunt. Daarbij kan worden gedacht aan Windows 7 of diverse Linuxdistributies. Helaas zijn er moederborden van bepaalde fabrikanten bekend waarbij dat niet kan. Bij op ARM gebaseerde systemen, zoals tablets, kan Secure Boot in elk geval niet worden uitgeschakeld, en is er geen 'custom mode'.




Geldige openbare sleutels worden opgeslagen in de signature database (db), terwijl herroepen (ongeldige) openbare sleutels worden opgeslagen in de revoked signature database (dbx).

Naast de Platform Key zijn er speciale sleutels met de naam Key Enrollment Key of ook wel Key Exchange Key (KEK). Deze zijn nodig voor het bijwerken van de signature en revoked signature databases. De KEK's worden opgeslagen in een eigen database, de KEK-database. De PK kan worden gebruikt voor het ondertekenen van nieuwe KEK's in de KEK-database of voor het uitschakelen van Secure Boot. Ook een fysiek aanwezige gebruiker kan dat doen via het firmwaremenu zonder de PK te gebruiken. Alle drie de databases worden door de fabrikant in het NVRAM van de firmware geplaatst.

Op computers die voor Windows 8 zijn gecertificeerd, staat Secure Boot al in de standaardmodus, waarbij de Platform Key van Microsoft in de signaturedatabase is opgeslagen. Dat betekent dat alleen nog besturingssystemen en drivers die met de sleutel van Microsoft zijn ondertekend, gestart kunnen worden. Microsoft heeft in de KEK-database een eigen KEK opgenomen, zodat het in de toekomst nieuwe besturingssystemen (Windows 10!) aan de signaturedatabase kan toevoegen.

## UEFI, Secure Boot, GPT en Linux

Windowsgebruikers hoeven zich over UEFI en wat dies meer zij geen zorgen te maken. Microsoft zorgt er immers wel voor dat UEFI past bij Windows en omgekeerd.

Hoe Linux omgaat met deze nieuwe UEFI-systemen, in het bijzonder Secure Boot, en welke gereedschappen Linux ervoor biedt, is het onderwerp van een volgend artikel. Het is met name interessant welke oplossingen er zijn gekozen om van Secure Boot gebruik te kunnen maken in plaats van het uit te schakelen.

# Henk van Andel

## erelid van HCC en CompUsers

René Suiker

*Bloemen voor erelid Henk van Andel, overhandigd door Clemens Schellens (l), de huidige voorzitter.*

We schreven al eens eerder, tijdens onze Algemene Ledenvergadering in april 2014 hebben we Henk van Andel erelid willen maken van CompUsers. Dat kon echter alleen als de moedervereniging daarin meewerkte. Op dat moment kregen we een mondelinge toezegging van Arda Gerkens, de toenmalige directeur.
Echter, formeel kon dat niet, omdat volgens de statuten van dat moment alleen de ledenraad van de HCC daarover kan oordelen en beslissen. Zo hing het erelidmaatschap van Henk van Andel, hoewel de bedoelingen helder waren, toch nog enige tijd in de lucht.

*Met de complimenten van de HCC, overgebracht door Arda Gerkens, directeur HCC*

Maar op 29 november 2014 heeft de ledenraad Henk van Andel alsnog formeel benoemd tot erelid van de HCC en daarmee ook van CompUsers.

Uiteraard feliciteren wij Henk hier van harte mee. Hij heeft onze vereniging jarenlang met veel energie en enthousiasme geleid. Hij is HCC-lid van het eerste uur (lidnummer 176) en vervult al meer dan 30 jaar bestuurlijke functies binnen de vereniging.

Ook nu nog is hij actief met o.a. onze GigaHits, maar we respecteren het dat Henk het een beetje rustiger aan wil gaan doen.