Vereniging van fabrikanten en gebruikers standaardiseert voor nieuwe markten

Multimediakaart naar UMTS-telefoon

UMTS is niet dood!

Voor een verwijderbaar opslagmedium met flitsgeheugen en een controller zijn talloze toepassingen te bedenken, vooral als het uitwisselbaar is tussen verschillende apparaten van verschillende fabrikanten. De MultiMediaCard Association probeert dit te bereiken door open standaarden te ontwikkelen. Vooral in de nieuwe generatie mobiele telefoons zal MMC doorbreken, aldus Executive Director Andy Prophet.

Om te beginnen: het 'universal mobile telephone system' is niet dood! Maar het heeft wel minimaal een vertraging opgelopen van zo'n twee jaar. Wat Europa betreft is er voor 2004 geen uitrol van betekenis te verwachten, aldus EMC senior research analiste Liz Hall. De uitbouw van de dit jaar begonnen proeven is echter vooral een kwestie van geld, zo vertelde zij op het door IBC georganiseerde UMTS 2003 Deployment Congress op 11 en 12 juni in Amsterdam.

Achter de schermen wordt er wel degelijk hard gewerkt aan de derde generatie (3G) mobiele

Andy Prophet, directeur van de MultiMediaCard Association: „In de zakelijke sfeer is beveiliging van de gegevens van groot belang".

telefonie en zeker ook aan de ontwikkeling van handsets. Een van de bedrijven, bijvoorbeeld, die een referentie-implementatie ofwel hardwareplatform heeft voor UMTS-telefoons is Texas Instruments. En Nokia is in juni 2003 al begonnen met de verscheping van de eerste 3G handsets voor de Europese en Aziatische markten.
De invoering van deze nieuwe technologie en bijbehorende diensten heeft ook gevolgen voor andere sectoren in de elektronica. Zo is een van de neveneffecten van sneller mobiel dataverkeer een toenemende behoefte aan geheugen in de handsets en dat is de reden dat ook de MultiMediaCard Association op het UMTS-congres aanwezig was. Een MMC is een verwijderbare 'solid state' geheugenkaart met controller en de MMCA is een vereniging van fabrikanten en gebruikers die daarvoor standaarden ontwikkelt.
Multimediaakaarten, zoals de vergelijkbare SD, Memory Stick en Compact Flash, worden tot nu toe vooral gebruikt in digitale fotografie en in videocamera's en PDA's, maar verreweg de grootste groei wordt verwacht in cellulaire telefoons. Het gaat dan om zo'n 150 miljoen stuks in 2005 - grote fabrikanten waaronder Nokia, Siemens en Motorola leveren thans modellen met MMC insteekgleuven. Inmiddels heeft de MMCA ongeveer honderd leden waaronder Eastman Kodak, Hewlett Packard, Infineon, SanDisk, Siemens, Nokia, Renesas (v/h Hitachi en Mitsubishi) en Samsung Electronics.
Vanwege een vergadering van de MMCA een dag later was ook Executive Director Andy Prophet in Amsterdam en Elektronica sprak op het UMTS-congres met deze voorman van de in 1998 opgerichte vereniging.

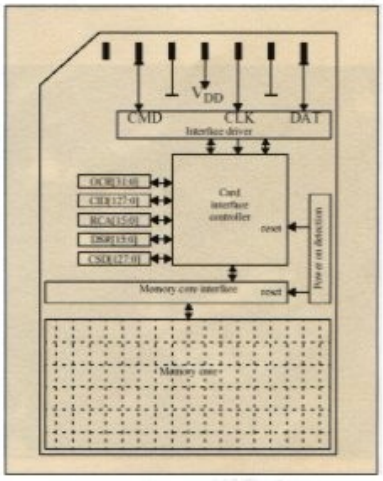
Geen Smart Card

De vraag of een multimediakaart een soort smart card is wuift Andy Prophet achteloos weg: „Een smart card is een plastic kaart en heeft heel andere toepassingen. Een multimediakaart is echt bedoeld voor gegevensopslag en kan in in ROM, OTP- (One Time Programmable) of MTP- (Many Times Programmable) versies worden uitgevoerd. Een spelletje dat je koopt voor een PDA of mobieltje zal bijvoorbeeld in ROM zijn opgeslagen. Voor het downloaden van muziek of het maken van foto's zul je flitsgeheugen gebruiken. Idem voor het hanteren van gegevens in een mobiele werksituatie, denk aan vertegenwoordigers, onderhoudsmonteurs en dergelijke. Een MMC is ongeveer zo groot als een postzegel en daarmee ook veel kleiner dan een smart card."
Toch heeft een MMC met zijn seriële datalijn en zijn duidelijk gespecificeerde interface veel overeenkomsten met een smart card. Dat lijkt nog meer het geval bij de beveiligde Secure MultiMediaCard. Die heeft net als een smart card een potentiële toepassing in elektronische en mobiele betalingen. Andy Prophet hierover: „Er bestaan een aantal variaties. Van de originele 7-pens kaart is inmiddels ook een 'reduced size' versie (RS-MMC) in omloop die echter met een hulpstuk ook in een normale insteekgleuf past. Maar inmiddels is er ook een 13-pens 'High-Speed MultiMediaCard' (HS-MMC) met een 4-bit of 8-bit databus. Alle kaarten gebruiken een interne klokfrequentie voor gegevensoverdracht en de HS-MMC kan met 52 MHz in de 8-pens versie dus 52 MB/s verwerken."

„Daarnaast is er echter ook een beveiligde variant, de SecureMMC, die ook mogelijkheden biedt voor elektronische handel en andere financiële transacties. Vooralsnog zien we daarvoor een toepassing in DRM (Digital Rights Management) ofwel de bescherming van 'content'. Een MMC is primair ontworpen om als opslagmedium te fungeren. Je hebt nu bijvoorbeeld stadsgidsen voor Parijs, Londen en Rome voor de Palm handcomputer die op een multimediakaart staan en die je dus zo kunt insteken. Combinatie met GPS is ook een toepassing van MMC - verschillende van onze leden doen in navigatie van schepen, auto's en met name ook huurauto's. In de zakelijke sfeer: verkopers van BMW gebruiken multimediakaarten om op kantoor klantgegevens in te laden en die vervolgens op locatie door de mobiele telefoon bij te werken.
Bij een dergelijk gebruik is uiteraard de beveiliging van de gegevens van belang en SecureMMC is verreweg het beste op dat gebied."

Beveiliging

In een artikel [1] in IEEE MultiMedia 'Can We Ever Charge Napster Users?' wordt het gebruik van die beveiliging voor DRM (Digital Rights Management) nader uitgelegd.
Het systeem staat bekend als 'Super Distribution Scheme' en gebruikt zowel symmetrische als asymmetrische versleuteling. Bij de laatste, PKI ofwel Public Key Infrastructure, kan iedereen een bericht sturen over een onbeveiligd kanaal door gebruik te maken van een zogenoemde publieke sleutel van de ontvanger. Dat bericht kan vervolgens alleen worden ontcijferd met een andere sleutel die alleen de ontvanger kent, de privésleutel. Dit PKI is verreweg het beste maar heeft als nadeel dat het veel rekentijd kost en dus minder geschikt is voor grote bestanden.
De digitale inhoud zelf, muziek bijvoorbeeld, wordt dus in dit 'super distributie schema' versleuteld met een symmetrische sleutel, die gelijk is voor verzender en ontvanger.
Doorgifte hiervan wordt nu verzorgd door de multimediakaart. Die krijgt een unieke publieke sleutel waarmee de server de symmetrische sleutel, gekoppeld aan een licentie, kan versturen. Alleen de MMC met dat unieke PKI-sleutelpaar kan met de ontcijferde symmetrische sleutel nu de inhoud ontcijferen die bijvoorbeeld al eerder op een onbeveiligd gedeelte van de kaart is opgeslagen. Alle sleutels zelf en de licentie bevinden zich in een TRM (Tamper Resistant Module) op de kaart.



De MultiMediaCard-architectuur.

Vervolgens heeft, in het geval van muziek, ook het afspeelapparaat een publieke en privé-sleutel toegewezen gekregen. De MMC versleutelt nu de symmetrische sleutel van de 'content' met de publieke sleutel van de speler die dus als enige die boodschap kan ontcijferen. Met die ontcijferde sleutel kan de van de kaart afgehaalde muziek nu worden afgespeeld, en dus alleen door dat afspeelapparaat met die unieke PKI-sleutels.
In Japan wordt dit distributie systeem onder de naam 'Keitade-Music' gebruikt om 'peer to peer' muziek te leveren over het mobiele-telefonienetwerk. Maar er zijn meer dan 2000 'inhoud pakketten' beschikbaar, waaronder lessen in vreemde talen en meezingen op tekst en muziek (karaoke), en het principe is ook geschikt voor andere media zoals CD en DVD. De SecureMMC verzorgt hier dus de 'Digital Rights Management' en fungeert steeds als intermediair tussen leverancier en consument. De SecureMMC doet ook zelfstandig het cryptografische rekenwerk.

Vrij van licentie

Als met UMTS ook in Europa een soort 'Keitade-Music' opgezet kan worden zou dat natuurlijk een enorme markt opleveren en toepassing van SecureMMC sterk bevorderen.
„Tegen 2006 zal een derde van de 400 miljoen dan verkochte cellulaire telefoons in de een of andere vorm een MMC gebruiken," zegt Andy Prophet.
„Dat wil niet zeggen dat we digitale camera's moeten vergeten, maar het grootste volume zal in mobiele telefoons omgaan. De maximale capaciteit van MMC is nu nog 256 MB maar binnen een half jaar zullen we al op 1 GB zitten en daarna gaat het naar 4 GB. En de kosten per MB zullen navenant dalen de komende jaren.
Het grote voordeel van de MultiMediaCard Association is verder dat onze standaarden licentievrij geïmplementeerd mogen worden en dat vermelding van onze merknaam niet verplicht is.
Een MMC kaart kan in de winkel dus verkocht worden als een Nokia of een Kodak kaart of onder elke andere gewenste merknaam. Voor de marketing van een consumentenproduct is dat een groot voordeel."

Literatuur

1) Kenji Taima, 'Can We Ever Charge Napster Users?', IEEE MultiMedia Volume 9, Number 4, October-December 2002

Inl.: www.mmca.org