

# WHITEPAPER SMARTPHONES / OF BETER GEZEGD: MOBILE DEVICES

## SERIOUS BUSINESS FOR ICT MANAGERS

*Producenten van mobiele devices spelen meer en meer in op de gebruikersbehoefte om communicatie zo goed mogelijk aan te laten passen aan onafhankelijkheid van tijd, plaats en moment. Ieder moment van de dag, ongeacht welke locatie en verbinding wenst de gebruiker zijn werkzaamheden uit te voeren, met een device wat passend is in de situatie waarin hij/zij zich bevindt. Of dit nu een vaste werkplek, laptop, tablet, smartphone of GSM is, deze verschillende devices stellen door hun grote variëteit aan mogelijkheden, in beheersoptiek steeds meer eisen aan de ICT-organisatie. Daarnaast stellen de eindgebruikers hun ICT-afdeling ook op de proef met het ongelimiteerde gebruik van mobiele (messaging-) applicaties, die vrijelijk kunnen worden gedownload van online applicatieportals. Hoe kunnen instellingen, bedrijven of organisaties deze uitdaging doorstaan? Hoe kan een ICT-organisatie flexibel omgaan met deze ontwikkelingen, zonder het hoofd te bieden aan een vastliggend ICT-beleid? Hoe kan veilige communicatie en security op deze mobiele devices worden voorzien zonder eindgebruikers gebruiksgemak te ontnemen?*

*In deze whitepaper leest u als IT, Telecom of Facility manager en -afdeling hoe u deze faciliteiten kunt aanbieden, beheren en met succes blijven voorzien.*



## Trends en ontwikkelingen

Naast de versnelde ontwikkeling van mobiele devices, neemt het explosieve gebruik van deze devices onder medewerkers een enorme vlucht en stelt menig bedrijf voor organisatorische vraagstukken. Buiten het verhoogd gebruik van support- en servicedesk-kanalen, wordt ook de expertise van deze kanalen op de proef gesteld. Gebruikersvragen verschuiven van incidenten, storingen en vragen rondom facturen naar integratievraagstukken met betrekking tot e-mailsynchronisatie, applicatiegebruik en Bring-Your-Own-Device vragen. Naast de verschuiving van kennis en kunde hieromtrent richting ICT-helpdesk, zorgt het gebruik van deze mobiele devices voor steeds meer vraagstukken die op ICT-management niveau beantwoord dienen te worden, zoals: hoe dient een bedrijf hier mee om te gaan? Welke afspraken worden hieromtrent gemaakt? Wat laat het ICT-beleid toe, en welke ontwikkelingen passen in het huidige ICT-beleid?



## De werkplek van vandaag

**Wat is nou eigenlijk een Smartphone?** Een veel gehoorde

vraag binnen ICT-organisaties en bedrijven, die door de ontwikkel-snelheid van mobiele telefoons meer dan gegrond is. Vanaf de eerste mobiele telefoons, die voorzieningen boden in de vorm van telefoongesprekken en korte tekstberichten via het GSM-platform, hebben er veel ontwikkelingen plaatsgevonden op het gebied van vorm, bediening en functionaliteit. Innervate typeert de huidige 'line-up' in mobiele devices als volgt: Basic GSM, Smartphone, Portable (Media) Tablet, Laptop. Vanuit het GSM-verleden zijn de extra functionaliteiten bij elkaar gevoegd in de Personal Digital Assistant (PDA), welke is gebaseerd op de toenmalige gebruikersbehoefte en -situatie, die digitale agenda-mogelijkheden bood naast het standaard-GSM-toestel waarmee gebeld werd. Na de samenkomst van deze twee apparaten in één, zijn er in de loop van de tijd steeds meer functionaliteiten aan toegevoegd, dat uiteindelijk resulteerde in de **Smartphone**. Hier zijn buiten convergentie van middelen en technieken cloudtoepassingen toegevoegd waar de Smartphone als endpoint naadloos in past. Vandaag de dag zijn Smartphones niet meer weg te denken in onze levens en maatschappij. Sterker nog, onder de consument en medewerker van vandaag vindt een migratie van behoefte plaats naar een device die de intelligentie van een smartphone combineert met een schermgrootte van een portable laptop, de **Tablet**. In deze *whitepaper* zullen wij ons focussen op de Smartphones en Tablets van vandaag.

Beide devices vinden hun kracht in een ontwikkeling die tien jaar geleden online heeft plaatsgevonden, namelijk communities. Communities, zoals fora, hebben de kracht om leden met gedeelde interesses kennis en ervaringen uit te laten wisselen. Ditzelfde geldt ook voor de cloudtoepassingen die op de devices beschikbaar komen. Veelal zijn dit applicaties, die door ontwikkelaars worden gemaakt, en via een online bereikbare applicatieportal, al dan niet betaald, kunnen worden gedownload. Denk hierbij aan de Android Market, Microsoft Marketplace, Apple AppStore, Blackberry Appworld of Nokia OVI-store. Door het aanbevelen van deze applicaties, veelal via social media zoals Twitter en Facebook, door medegebruikers, worden applicaties met groot gemak geïnstalleerd en gebruikt. Dit brengt in bedrijfsoptiek een aantal nadelen met zich mee waar vooraf afspraken over gemaakt dienen te worden:

**Apps...Apps...Apps** De huidige smartphone kan niet zonder een eigen applicatie-marktplaats en de race om de meeste 'apps' wordt nu gelopen. Hierdoor heeft de gebruiker veel keuze, maar ziet vaak door de bomen het bos niet meer. Social Media biedt vaak hulp bij de keuze. Echter de vele applicaties met "vriendenadvies" leveren ook een potentieel gevaar omdat vaak niet duidelijk is wie de maker is en welke bedoeling deze heeft.

### 1. Gebruik van (betaalde) applicaties

Door het gemak van de applicatieportal is de 'probeerformule' voor eindgebruikers hoog. Ogenscheinlijk interessante applicaties kunnen met twee keuzes op het toestel worden geïnstalleerd. Maar welke applicaties laat het bedrijf toe wanneer het toestel in beheer is van de ICT-helpdesk? En wanneer een eindgebruiker een betaalde applicatie wilt downloaden, kan dat op zijn eigen rekening? Of dient hij dit te declareren bij het bedrijf?

### 2. Downloaden en controleren van applicaties

Doordat de ontwikkelsnelheid van de applicaties in de portal hoog ligt, en gebaseerd is op input van 'onbetrouwbare bronnen' is de controle op veiligheid van de applicaties bij het downloaden lastig te borgen vanuit ICT-optiek. Dit brengt risico's met zich mee op het gebied van de informatiebeveiliging. Applicaties verzamelen en versturen vaak 'onderhands' data naar externe servers. Door het vereisen van een antivirus-applicatie op het toestel kan dit ten dele worden tegen gegaan.

### 3. Versiebeheer en dataroaming applicaties

Naast de hoge ontwikkelsnelheid van de applicaties wordt continue, op basis van gebruikersfeedback, de applicatiefunctieiteit door ontwikkelaars bijgewerkt. Doordat deze applicaties hun update-cyclus automatisch uitvoeren, kan dit impact hebben op dataverbruik. Denk bijvoorbeeld ook aan de update van een applicatie in het buitenland. Dit kan tot onnodige kosten leiden en de helpdesk grijze haren bezorgen als het device erna niet meer werkt.

### 4. Beheer

Gebruikers willen steeds meer keuze in het type mobiele device. Door het brede palet aan devices zal ook beheer van de verschillende platforms hier rekening mee moeten houden. Daarbij is een goede aansluiting bij het bestaande ICT-beveiligingsbeleid zeer aan te raden. Vaak is asset-management wel ingericht op hardware en software, maar ontbreekt een duidelijke afgebakend data-beleid en worden simkaarten en de bijbehorende abonnementen regelmatig over het hoofd gezien.

#### Aandachtspunten voor Telecom:

#### Top Tien

1. Nummerportering/contract-overname
2. Nummerplan
3. Fiscale aspecten van vergoedingen
4. Split billing
5. Verborgene kosten door declaratie-proces
6. Handsfree bellen
7. Handhaving gebruik
8. Beveiliging
9. Kosten/budgetbeheer
10. SLA reparatie/vervanging

#### Telecommanagement

De mogelijkheden van telecommunicatiemiddelen zijn de laatste jaren sterk aan verandering onderhevig en enorm toegenomen. Het management (beheer en beleid) van alle communicatiemiddelen vraagt om een effectief telecombeleid. Efficiënte processen en adequaat leveranciersmanagement leiden tot transparantie in kosten en inzicht in performance. Toekomstige ontwikkelingen op het gebied van telefonie naar VoIP en Unified Communications en de enorme groei in smartphones vragen om een herijking van de processen en het ICT-beleid binnen een organisatie. Technisch is er veel mogelijk maar succes wordt na de implementatie sterk beïnvloed door effectief telecommanagement.

Het hebben van stuurinformatie over alle communicatiemiddelen met de

daarbij behorende rapportages over gebruik en kosten zijn cruciaal om verdere ontwikkelingen te kunnen ondersteunen, maar ook om innovatie te stimuleren.

## Dat netwerk, DPI, Wireless en VoIP

Het gebruik van smartphones heeft in de afgelopen twee jaar geleid tot een zeer forse stijging in het mobiele internetverkeer. Dit komt niet alleen doordat er meer smartphones zijn gekomen maar ook door het gebruik ervan. Over het algemeen verstuurt men minder sms-berichten en maakt daarvoor in de plaats meer gebruik van een online applicatie. Dit betekende dat verschillende providers een verdubbeling van het internetverkeer hebben geconstateerd ten opzichte van een jaar ervoor door het gebruik van smartphones. Met de komst van tablets verwacht men dat het dataverbruik vijf keer zo hoog zal liggen als met een smartphone. Ook het gebruik van tablets zal impact hebben op het verbruik van mobiele internet verbindingen via providers maar ook op draadloze netwerken binnen bedrijven.

Door de toename van mobiel internet is het van belang om de kosten voor dataverbruik in de hand te houden. Data bundels vallen nu vaak nog onder een 'fair use policy' of groepsbundel waardoor de kosten bij extreem dataverbruik niet hard oplopen. In de aankomende jaren zal hier mogelijk verandering in komen doordat providers hun data bundels en voorwaarden zullen aanpassen.

Providers willen de gebruikers eigenlijk afrekenen aan de hand van hun dataverbruik of diensten die zij afnemen op het internet. Doordat providers neutraliteit van het mobiele netwerk moeten waarborgen mag er geen controle plaatsvinden op een datastroom en kan er niet gefactureerd worden aan de hand van de diensten maar alleen door middel van dataverbruik. Echter om de verkeersstromen te managen controleren de verschillende providers het netwerkverkeer door middel van Deep Packet Inspection (DPI).



Smartphones kunnen verbinding maken met het internet via publieke internet toegangspunten of via een afgeschermd omgeving (APN) van telecommunicatie aanbieders. Daarnaast zijn er ook mogelijkheden om toegang tot het internet in eigen beheer aan te bieden op bepaalde locaties via Private GSM of draadloze netwerken. Al deze verschillende mogelijkheden hebben hun voor- en nadelen.

Om de kosten van smartphones in de hand te houden kan het van belang zijn om op alternatieve manieren spraak- en datasessies af te handelen. Dit wordt 'least-cost-routing' genoemd en is mogelijk door middel van de diverse toegangspunten alsmede door het installeren van software op smartphones. Hierdoor kan het bijvoorbeeld mogelijk worden om telefoongesprekken naar het buitenland altijd via het draadloze netwerk te laten verlopen en niet via het standaard mobiele netwerk van de telecommunicatie aanbieder.

De impact van smartphones op een draadloos netwerk binnen bedrijven is hoog, afhankelijk van de diensten die er aangeboden worden. Doordat men interne netwerken gebruikt kan men bijvoorbeeld het intranet en andere bedrijfsapplicaties toegankelijk maken.

## Security

De beveiliging van een smartphones behelst niet alleen de toegang tot de gebruikers interface maar ook de communicatie van en naar het device toe. Het beveiligingsbeleid dat voor smartphones wordt gebruikt moet onderdeel uitmaken van het ICT beveiligingsbeleid en moet gedragen, nagevolgd en uitgevoerd worden van Operationeel via Tactisch tot Strategisch niveau. Hierin kunnen onder andere wachtwoord karakteristieken worden afgesproken maar ook de voorwaarden waaraan toestellen moeten voldoen bijvoorbeeld een OS versie. Daarnaast moet vast worden

gesteld welke data er op een smartphone mag komen te staan. Hierbij kan het van belang zijn om bepaalde functies zwaardere/andere eisen toe te kennen met betrekking tot het gebruik van lokaal opgeslagen informatie op de smartphone. Denk hierbij bijvoorbeeld aan het verschil in impact wanneer een uitvoerende medewerker een smartphone verliest ten opzichte van een CEO.

Wanneer de smartphone en de data communicatie goed beveiligd is kan men de processen rond het beheer inregelen. Hierbij kan men denken aan het koppelen van een smartphone en de hoeveelheid devices die gekoppeld mogen worden aan één persoon. Het inrichten van bedrijfsprocessen over het aansluiten, vervangen en beëindigen van een smartphone en het bijbehorende abonnement is van groot belang om er zeker van te zijn dat een device niet in verkeerde handen valt. Wanneer verkeerde personen een toestel in bezit hebben kunnen zij eindeloos proberen toegang te krijgen tot de bestanden op het device en mogelijk ook tot het bedrijfsnetwerk.

**Naast het beveiligen van de data is het van belang dat de data ook gesynchroniseerd is en daarbij niet verloren gaat wanneer een smartphone kapot gaat. In veel gevallen gaat bij een defecte smartphone bedrijfsinformatie verloren die niet terug gehaald kan worden.**



Voor alle smartphones besturingssystemen zijn veel verschillende 'apps' beschikbaar waarmee de gebruiker extra mogelijkheden heeft of eenvoudiger toegang krijgt tot specifieke websites. Een app kan ook voor grote beveiligingsrisico's zorgen wanneer het toegang verleent aan derden of gegevens kopiëert buiten medeweten van de gebruiker om.

Het kan daarom van belang zijn om bepaalde apps niet toe te staan binnen een organisatie. Om dit te kunnen realiseren kan men gebruik maken van (Mobile) Device Management Software waarmee een smartphone volledig of gedeeltelijk beheerd kan worden. Afhankelijk van het besturingssysteem van de smartphone heeft men verschillende beheersmogelijkheden. Een van de mogelijkheden is het toestaan van applicatie of definiëren van een zwarte lijst zodat bepaalde applicaties niet geïnstalleerd kunnen worden. Tevens kan men vaak ook standaard software aanbieden voor de smartphone binnen een organisatie, dit kan handig zijn voor het aanbieden van telefoonboeken welke integreren met de interne telefonieomgeving van het bedrijf zelf, antivirussoftware of maatwerk applicaties.

De beveiliging van smartphones is afhankelijk van gebruikers alsmede van de ICT policy. Op basis van de gewenste mate van vertrouwelijkheid van de data kan een standaard oplossing (zoals een active sync koppeling) niet toereikend zijn. De hoogte van beveiliging tijdens het datatransport van en naar smartphone hangt samen met het gekozen ICT-beleid. Blackberries bijvoorbeeld, verbinden zich niet direct met de mailomgeving maar met een eigen Blackberry Enterprise Server die alleen beschikbaar is via het wereldwijde RIM netwerk. Windows, Android en iOS smartphones verbinden zich daarentegen over een beveiligde internetverbinding naar een mailomgeving. Deze verbinding kan men beveiligen door extra certificaten aan het apparaat toe te kennen. Hierdoor is de omgeving niet publiekelijk toegankelijk, maar wordt het door toepassing van certificaten voor zowel de eindgebruiker als de ICT-omgeving wel vele malen veiliger.

## Tablets

Sinds 2011 is de opkomst van de tablet zodanig geëvolueerd dat er geen sprake meer is van een niche-product, maar dat fabrikanten grote verscheidenheid aan tablets op de markt brengen. Veel organisaties zoeken nog naar mogelijkheden voor het inzetten van tablets, waarbij het beheer en kosten de belangrijkste rollen spelen. Maar ook

steeds vaker wordt er gekeken naar de mogelijkheden en de tijdwinst die te behalen is door het gebruik van tablets bij medewerkers. Het middel is namelijk perfect in te zetten voor document-reviewing en content-surfing, met de voordelen van cloud-toepassingen, waardoor deze net als een smartphone naadloos als een endpoint integreert in de informatievoorziening aan de eindgebruiker.

In de aankomende jaren zullen, getuige de groei van de tabletmarkt, steeds meer bedrijven tablets gaan produceren en zullen er ook meerdere besturingsystemen op de markt komen. Fabrikanten zullen zich bij de ontwikkeling van nieuwe tablets meer gaan richten op content-creation, dat is een gebrek dat bij de huidige tablets nog bestaat.

Het organisatorisch goed inrichten van het beheer van een tablet valt vaak tussen wal en schip. De oorzaak is te vinden in het feit dat er geen 'dedicated device managementpakketten' worden gebruikt en daarbij wordt er steeds vaker ook een simkaart in geplaatst waardoor de Telecom- en IT-domeinen met elkaar verbonden worden. Een tablet wordt daardoor vaak onder de Telecombeleidsstukken geplaatst, vanwege het feit dat er een data-abonnement nodig is in verband met de benodigde internet-verbinding.

Ook is het organisatorische gezien een uitdaging om bij het verstrekken van tablets op een goede manier in te richten op profielniveau. Het device wordt vaak niet verstrekt vanuit de ICT organisatie, maar vanuit consumeratie, met andere woorden: door de medewerkers zelf meegebracht.

**Tablets in alle vormen en maten** Tablets zijn er in alle vormen en maten en het verschil met een Smartphone is vaak erg klein. ABI Research<sup>®</sup> heeft in hun marktonderzoeken aangegeven dat een mediatablet 5" of groter is, Over-The-Air kan updaten, accu vriendelijk is, directe interactie met de gebruiker kan aangaan zonder opstarttijd en Wifi heeft. Bluetooth en 3G zijn optioneel. Het verschil in gebruik zit in het consumeren, creëren en mobiel werken. Er vindt geen kanibalisatie plaats door de tablet, maar eerder een natuurlijke vervanging. Ook is de vraag niet **OF** er vervangen wordt, maar **WANNEER?**

## Bring Your Own Device / Choose Your Own Device

Het gebruik van smartphones binnen bedrijven en organisaties hangt vaak samen met een tweetal punten, namelijk: de aantrekkelijkheid als werkgever en Het Nieuwe Werken.

Het beschikbaar stellen van smartphones binnen een organisatie is voor veel jonge medewerkers belangrijk omdat zij gewend zijn om met moderne communicatiemiddelen te kunnen werken. De komst van smartphones en de kosten die daarbij horen zijn hierdoor onderdeel geworden van mogelijke contractsonderhandelingen en het behouden van werknemers binnen een organisatie. Hierbij speelt de HR afdeling een belangrijke rol. Zij moeten goed op de hoogte zijn van de mogelijkheden, maar ook van de consequenties en impact die het bijvoorbeeld heeft voor de afdracht van gelden die over gegenereerd loon aan de Belastingdienst betaald moeten worden.

Zo veel verschillende functies er binnen een bedrijf of organisatie zijn, zo groot is de diversiteit aan smartphones. Hierdoor is er altijd wel een smartphone die aansluit bij de wensen en eisen van een medewerker, maar ook net dat ene toestel wat niet in het assortiment zit of niet werkt.

Binnen een organisatie moet er middels profilering duidelijk aangegeven worden welke medewerkers in aanmerking komen voor smartphones en/of tablets. Dit beleid moet ook gedragen worden binnen een organisatie zodat er niet via allerlei achterdeuren toch apparaten en abonnementen afgesloten en gedeclareerd worden.

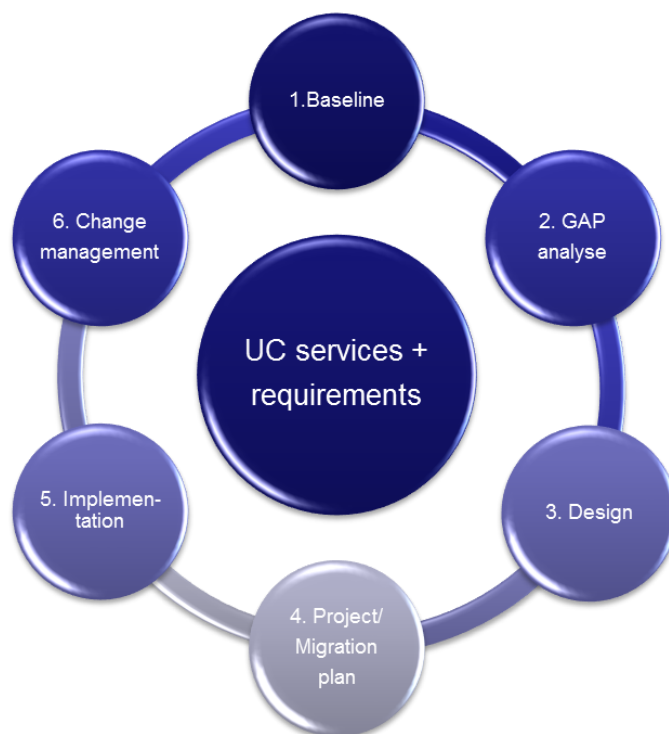
## Stappenplan: implementatie van mobile devices

Zoals duidelijk is geworden in het voorafgaande vereist een succesvolle implementatie van Mobile Devices binnen een organisatie een complex samenspel van een groot aantal onderdelen. Vrijwel altijd zal er een bepaalde installed-base van GSM-toestellen aanwezig zijn die in meer of mindere mate geïntegreerd zijn in de telefonie-omgeving. Tevens is de bestaande installed-base gegroeid op basis van de behoefte en wens aan mobiliteit en bereikbaarheid van de eindgebruiker. Meer dan eens ervaren wij dan ook dat er een brede selectie aan mobiele toestellen aanwezig is binnen een organisatie, met daaraan gekoppeld een complexe beheerorganisatie.

**Onze stelling is dan ook dat mobiele toestellen, in de breedste zin des woords, in elk geval een groot onderdeel uitmaken van de Unified Communications-omgeving van een klant.**

Afhankelijk van de communicatie-inrichting van de klant kan de mate van het gebruik van mobile devices als mobile-only of mobile-endpoint oplossing binnen een bedrijf worden gezien. Er zijn immers vaak basale of verregaande integraties terug te vinden aan zowel de voorzijde van de communicatie-inrichting, zoals vast-mobiel integratie / convergentie, als wel aan de achterzijde, met verschillende applicatie-integraties zoals Exchange, Sharepoint, etcetera.

Om dit complexe samenspel van nieuwe en reeds aanwezige elementen tot een goed werkend systeem te integreren is door Innervate een aanpak ontwikkeld die gebruik maakt van de inzichten op het gebied van ICT architectuur. De kern van deze Unified Communications-Roadmap bestaat uit een basismodel van een UC systeem, opgebouwd uit drie lagen, waarbij de noodzakelijke relaties zijn vastgelegd tussen services, applicaties en ICT infrastructuur. In onderstaande figuur is dit model sterk vereenvoudigd weergegeven. Door dit model als een template tegen een bestaande omgeving aan te houden wordt zichtbaar welke overlappings en hiaten er zowel op functioneel als technisch niveau liggen. Vanuit deze analyse kunnen bijvoorbeeld dan de noodzakelijke functionele en technische ontwerpen voor de inrichting van een veilig en een daadwerkelijk mobiele communicatieomgeving worden opgesteld.



## Waarom Innervate?

Innervate is een eredivisiespeler in het vakgebied van informatietechnologie en ICT infrastructuur. Onze diensten zijn gericht op advies, softwareontwikkeling en trainingen. De professionals van Innervate zijn allemaal spelers' met hun eigen specifieke expertise en praktijkervaring. Innervate kan de werkprocessen in uw organisatie geheel overzien en exact de puntjes op de 'i' zetten. Dit levert voor de klant een slimme oplossing op en 100% kans op een succesvol project, met name op het gebied van het integreren en beheren van **Mobile Devices**.

### Voor meer informatie:

#### **Innervate**

Aziëlaan 14  
6199 AG Maastricht-Airport

#### **Innervate Midden Nederland**

De Corridor 21 A  
3621 ZA Breukelen

**T** +31 (0) 43 358 1880

**E** [info@innervate.nl](mailto:info@innervate.nl)

**W** [www.innervate.nl](http://www.innervate.nl)

Volg ons op **LinkedIn**:

<http://nl.linkedin.com/innervate>

Volg ons op **Twitter** :

**#InnervateNL**

Volg ons op **Facebook**:

**Innervate NL**

## **Nawoord**

Deze whitepaper is opgesteld door Sven Kort, Gerjan Eghuizen en Bart Martens, gebaseerd op de project- en onderzoekservaring op het gebied van Unified Communications, Telecom Management en Mobiel beheer.