A1 SMART CLIENT

Benutzerhandbuch

Einführung

Dieses Handbuch begleitet Sie bei der Installation und Konfiguration des A1 SMART CLIENTSMART CLIENT.

Die Mobilkom Converged Network Platform Architektur (CNP) bietet ein sicheres Hochgeschwindigkeits-Funkdatennetz, welches das WLAN nahtlos mit Mobilkom-Netz verbindet. Die CNP Architektur bietet Carrier-class Service durch die SMART CLIENT Software, die WLAN oder GPRS Karte Ihres Notebooks, und einen Access Point (AP). Der A1 SMART CLIENT bietet Benutzerfreundlichkeit, Zuverlässigkeit und Datenschutz. Access Points stellen einen transparenten, drahtlosen IP Pfad zwischen Internet und dem SMART CLIENT, der auf Ihrem Notebook installiert ist, zur Verfügung.

Sicherheit

Alle Daten eines authentifizierten Benutzers werden während der Übertragung mit 128-Bit Advanced Encryption Standard (AES) verschlüsselt. Dadurch wird eine sichere Verbindung zwischen dem auf dem Computer des Kunden installierten SMART CLIENT und dem WSC hergestellt. Die Verschlüsselung schützt sowohl den Computer des Kunden vor Attacken anderer Computer im WLAN, als auch die Daten des Kunden gegen unerlaubte Zugriffe.

Der SMART CLIENT bietet weiters eine einfache Schnittstelle, mit Hilfe derer sich die Kunden zum Netz verbinden und ihre Roaming-Möglichkeiten kontrollieren können. Die CNP Architektur unterstützt Subscriber Identity Module (SIM) Authentifizierung.

Nahtlose Handovers

Wenn Benutzer eine Verbindung herstellen, können sie innerhalb des Hotspots von einem AP in einen anderen wechseln. Typischerweise nimmt die Signalstärke des AP bei Annäherung des Benutzers zu. Wenn das Signal des AP, in dessen Richtung sich der Benutzer bewegt, stärker wird, als das Signal des AP, mit dem er verbunden ist, schaltet die drahtlose Verbindung automatisch und transparent auf den AP um, der sich näher beim Notebook des Benutzers befindet. Dieses Umschalten der Verbindung zwischen APs wird Handover genannt und von der Software der WLAN Karte durchgeführt. Die SMART CLIENT Software führt diesen Handover für den Benutzer nahtlos durch, da sie auf einer höheren Schicht arbeitet, als die Software der WLAN Karten. Für den Benutzer gibt es keine Wartezeiten oder Unterbrechungen während des Handover zwischen den APs.

Sichere Paketvermittlung im öffentlichen Raum

Da WLANs, besonders, wenn sie sich an öffentlichen Orten befinden, von Natur aus anfällig für Sicherheitsattacken sind, wendet der CNP eine Firewall-Methode auf Benutzerebene an, welche jeglichen Peer-to-Peer Traffic von anderen WLAN Benutzern verhindert. Dadurch werden die Benutzer vor Angreifern im selben WLAN geschützt.

Auf Netzwerkseite überträgt der CNP den drahtlosen Traffic des Kunden mittels eines verschlüsselten PPP Tunnels. Dieser Tunnel schützt nicht nur die Kundendaten vor dem Abhören sondern auch das Core-Netz des Mobilbetreibers vor unberechtigten Zugriffen.

Gegenseitige Authentifizierung

Das CNP Netz ermöglicht in Verbindung mit der SMART CLIENT Software die gegenseitige Authentifizierung unter Verwendung der bestehenden SIM Berechtigungen des Kunden. Dank der gegenseitigen Authentifizierung können sich verbrecherische WLAN Netze nicht als berechtigte WLAN Systeme ausgeben. Die gegenseitige Authentifizierung verhindert auch, dass sich Teilnehmer in das Netz Dritter einloggen, wo die Datensicherheit eines Kunden gefährdet sein könnte. Ebenso verhindert sie auch Angriffe zum Zweck des "Service-Diebstahls" durch unberechtigte Benutzer.

VPN Unterstützung

Die CNP Architektur unterstützt bestehende VPN Clients. Der CNP schließt die VPN Unterstützung ein, da der WSC IP Pakete transparent tunnelt, ohne Änderung der IP Paket-Information.

Selbststartend

Wenn ein Kunde den Versorgungsbereich des CNP betritt, werden ihm die verfügbaren Services durch das A1 WLAN Access Portal vorgestellt. Dieses Portal ermöglicht einem neuen Benutzer das Herunterladen und Installieren der SMART CLIENT Software auf seinem Gerät.

Überblick

Die SMART CLIENT Software verbindet End-User mit dem Mobilkom-Netz Um sich über WLAN zu verbinden, benötigen End-User lediglich ein Notebook, das mit einem SIM Kartenleser oder einer WLAN (oder GPRS) Karte ausgestattet ist. Die SMART CLIENT Software verbindet sich mit dem SIM Kartenleser und liest die SIM Information. Die SMART CLIENT Software verwendet die in der SIM Information enthaltenen Berechtigungsnachweise, um den Benutzer am Netz zu authentifizieren. Sobald der Benutzer authentifiziert ist, wird ihm der Zugang zum Internet gewährt.

SMART CLIENT Features

Der SMART CLIENT wickelt Verbindungsmanagement, Profilmanagement und Verbindungskonfigurationen für alle Verbindungen zum Netz ab.

Verbindungsmanagement

Das Verbindungsmanagement ermöglicht es dem Benutzer, die Parameter für eine bestimmte Verbindung zu spezifizieren. Das Verbindungsmanagement ermöglicht es dem Benutzer, folgende Aktivitäten durchzuführen:

• den AP festlegen, zu dem man sich verbinden will

• die Verschlüsselung festlegen, die man bei der Verbindung verwenden will

• Das Profil festlegen, das der SMART CLIENT bei der Verbindung verwenden soll (optional)

Profil Management

Das Profil Management ist eine Zusammenstellung von voreingestellten Konfigurationsparametern für eine bestimmte Verbindung. Das Profilmanagement ermöglicht es dem Benutzer, folgende Aktivitäten durchzuführen:

• Profile erstellen, ändern und löschen

• einen Profilnamen festlegen

• festlegen, ob für die jeweilige Verbindung eine Verschlüsselung angewandt wird, oder nicht

• die Art der Authentifizierung für jedes Profil festlegen

• den Access Point Namen (APN) festlegen, zu dem man sich verbinden will und die von seinem Service Provider geforderten Authentifizierungsparameter zu konfigurieren.

Konfiguration

Die Konfiguration ermöglicht dem Benutzer Folgendes:

• Verschlüsselungen aktivieren und deaktivieren

• die jeweilige Dauer der Connection Timeouts festsetzen

• die Protokollierung ein- und ausschalten und den Standort des Log File angeben

SMART CLIENT Betrieb

Der SMART CLIENT bietet folgende Möglichkeiten:

• Datensicherheit unter Verwendung von Verschlüsselung

• leicht zu bedienende GUI Schnittstelle

• Verbindungen zum Internet zu öffnen und zu schließen

• Verbindungsversuche zu protokollieren

• Profile für alle Verbindungen zu erstellen

• die Performance jeder Verbindung zu überwachen

Installation und Konfiguration Ihrer A1 SMART CLIENT Software

Dieses Kapitel beschreibt die benötigte Hardware und Software, um

SMART CLIENT auf Ihrem Notebook ausführen zu können und führt Sie durch die nötigen Schritte, um Ihr Notebook auf die Verbindung mit vorzubereiten. Dieser Prozess besteht aus drei grundlegenden Aufgaben:

• Installation und Konfiguration Ihrer WLAN Karte

• Konfiguration Ihrer TCP/IP Einstellungen

• Herunterladen und Installation der SMART CLIENT Software

Hardware und Software Anforderungen

Um verbinden zu können, muss Ihr Notebook folgende

Voraussetzungen erfüllen:

• Intel x86 kompatibel mit PCMCIA Slot oder eingebauter WLAN Karte

• Universal Serial Bus (USB) port.

• mindestens 10 Megabytes verfügbarer Speicherplatz

• Microsoft Windows 2000, Service Pack 2, oder Microsoft Windows XP

• SIM Kartenleser (z.B. USB, PCMCIA, oder eingebauter SmartCard Leser)

• SIM Karte (muss in den SIM Kartenleser eingeführt werden)

• Eine 802.11b-fähige PCMCIA WLAN oder GPRS Karte

Unterstützte WLAN-Karten

Die folgende Tabelle listet alle WLAN Karten auf, die unter Windows XP und Windows 2000 funktionieren. Sollte Ihre Karte nicht auf der Liste sein, könnte sie jedoch trotzdem unterstützt werden.

WLAN Karte	**Windows XP**	**Windows 2000**
Alcatel Speed Touch PC Card	X	
Avaya Wireless PC Card	X	X
Belkin F5D6020 PC Card	X	

Buffalo Wireless PC Card	X	
Cisco Aironet 340	X	X
Cisco Aironet 350	X	X
Compaq WL110 PC Card	X	
Dell TrueMobile 1150 embedded	X	
Dell TrueMobile 1150 PC Card	X	
D-Link DWL-650	X	X
D-Link DWL-650+	X	X
Enterasys RoamAbout 802.11 DS	X	
HP hn220W PC Card	X	X
HP Wireless embedded	X	
IBM High Rate Wireless embedded	X	
IBM High Rate Wireless PC Card	X	
Intel PRO/Wireless 2011B	X	
Legend Joynet WLAN PC Card	X	
Legend Skyward PC Card	X	
LinkSys WPC11 ver.2/3	X	X
Lucent WaveLan Gold	X	X
Lucent WaveLan Silver	X	X
NCR Wavelan PC Card	X	

NEC Corp Wireless PC Card	X	
NETGEAR MA401	X	X
Proxim / Lucent ORiNOCO Gold	X	X
Proxim / Lucent ORiNOCO Silver	X	X
Proxim ORiNOCO Gold	X	X
Proxim ORiNOCO Silver	X	X
Proxim ORiNOCO USB Gold	X	X
Samsung MPCI 64-Bit	X	
Samsung PC-Card 64-Bit	X	
Siemens I-Gate 11M PC Card	X	
SMC 2632W V.2	X	X
SMC 2632W V.3	X	X
Sony PCWA-C150S PC Card	X	X
Sony Vaio embedded	X	
Toshiba Wireless embedded	X	
Toshiba Wireless PC Card	X	
Westell 802.11b PC Card	X	

Zusätzlich unterstützt der SMART CLIENT die folgenden drei GPRS Karten unter Windows 2000 und Windows XP.

GPRS Karte	**Windows XP**	**Windows 2000**
Nokia D211 combo GPRS/WLAN card	X	X

Sierra Air Card 750	X	X
Option GlobeTrotter	X	X

Bevor Sie Beginnen

Bevor Sie mit der Installation der SMART CLIENT Software auf Ihrem Notebook beginnen, stellen Sie sicher, dass Sie die folgenden vorbereitenden Tätigkeiten abgeschlossen haben:

• Schließen Sie alle Anwendungen bis auf einen Browser

• Stellen Sie sicher, dass auf der Festplatte mindestens zwei Megabytes freier Speicherplatz zur Verfügung stehen

Wenn nicht genügend freier Speicherplatz auf der Festplatte zur Verfügung steht, kann die Installation misslingen.

• Deaktivieren Sie alle VPN Verbindungen auf Ihrem Notebook.

Sie können die VPN Verbindung nach der Installation der SMART CLIENT Software wieder aktivieren.

• Installieren Sie eine der unterstützten WLAN Karten auf Ihrem Notebook gemäß den Instruktionen des Herstellers.

1: Konfiguration Ihrer WLAN Karte

Folgen Sie den, in der Ihrer Betriebssystemversion, beschriebenen Schritten, um Ihr Notebook für eine WLAN Verbindung ins Internet zu konfigurieren:

1.1 Konfiguration von WLAN Cards für Windows 2000:

1. Klicken Sie mit der rechten Maustaste auf das **Arbeitsplatz** Icon auf dem Desktop Ihres Computers und wählen Sie **Eigenschaften** . Darauf erscheint das Fenster **Systemeigenschaften**.
2. Wählen Sie die Registerkarte **Hardware** im Fenster **Systemeigenschaften**
3. Klicken Sie Sie auf den **Geräte-Manager** Button. Jetzt erscheint das Fenster **Geräte-Manager.**
4. Öffnen Sie im Fenster **Geräte-Manager** den Ordner **Netzwerk-Anschlüsse** und ermitteln Sie den Treiber für Ihre WLAN-Karte (Das Beispiel in der obigen Abbildung zeigt den Linksys WLAN card driver).

5. Doppelklicken Sie auf den Eintrag für Ihre WLAN-Karte. Jetzt erscheint das Fenster **Eigenschaften** für diese WLAN-Karte.
6. Die Art der Darstellung der Konfigurationseinstellungen für die WLAN Karte in der Dialogbox kann je nach Kartenhersteller unterschiedlich sein. Die folgenden drei Haupteinstellungen für Ihre Karte müssen Sie jedoch ordnungsgemäß konfigurieren, damit Ihre Karte richtig funktioniert.

- **WEP** Verschlüsselung muss abgeschaltet sein
- SSID oder **ESSID** muss auf den Default APN Namen eingestellt sein, der von Ihrem Service Provider zur Verfügung gestellt wird.
- Network type oder mode muss auf **Infrastructure** eingestellt sein (anstatt Adhoc).

Informationen über spezifische WLAN Card Konfigurationseinstellungen entnehmen Sie bitte der Herstellerdokumentation.

1.1 Konfiguration von WLAN Cards für Windows 2000:

1. Klicken Sie mit der rechten Maustaste auf das **Arbeitsplatz** Icon auf dem Desktop Ihres Computers und wählen Sie **Eigenschaften** . Darauf erscheint das Fenster **Systemeigenschaften**.
2. Wählen Sie die Registerkarte **Hardware** im Fenster **Systemeigenschaften**
3. Klicken Sie Sie auf den **Geräte-Manager** Button. Jetzt erscheint das Fenster **Geräte-Manager.**
4. Öffnen Sie im Fenster **Geräte-Manager** den Ordner **Netzwerk-Anschlüsse** und ermitteln Sie den Treiber für Ihre WLAN-Karte (Das Beispiel in der obigen Abbildung zeigt den Linksys WLAN card driver).
5. Doppelklicken Sie auf den Eintrag für Ihre WLAN-Karte. Jetzt erscheint das Fenster **Eigenschaften** für diese WLAN-Karte.

Die Art der Darstellung der Konfigurationseinstellungen für die WLAN Karte in der Dialogbox kann je nach Kartenhersteller unterschiedlich sein. Die folgenden drei Haupteinstellungen für Ihre Karte müssen Sie jedoch ordnungsgemäß konfigurieren, damit Ihre Karte mit dem CNP richtig funktioniert.

- **WEP** Verschlüsselung muss abgeschaltet sein
- SSID oder **ESSID** muss auf den Default CNP AP Namen eingestellt sein, der von Ihrem Service Provider zur Verfügung gestellt wird.
- Network type oder mode muss auf **Infrastructure** eingestellt sein (anstatt Adhoc).

Informationen über spezifische WLAN Card Konfigurationseinstellungen entnehmen Sie bitte der Herstellerdokumentation

1.2 Konfiguration von WLAN Cards für Windows XP

Die Schritte zum Konfigurieren Ihrer WLAN Card unter Windows XP sind dieselben Für jede unterstützte Karte. Gehen Sie folgendermaßen vor, um jede beliebige vom CNP Unterstützte WLAN Card unter Windows XP zu konfigurieren:

1. Klicken Sie auf das Icon **Wireless Connection** in der Task Leiste rechts unten am Bildschirm.
2. Abhängig davon, ob Sie gerade eine Verbindung zu einem Mobilnetz APN haben, sehen Sie eine von zwei verschiedenen Dialogboxen.
3. Wenn Sie keine Verbindung zu einem AP haben, erscheint die Dialogbox **Mit dem drahtlosen Netzwerk verbinden**, welche alle APs im Bereich Ihrer WLAN Card zeigt.
4. Klicken Sie auf **Erweitert**.
5. Wenn Sie gerade eine Verbindung zu einem Mobilnetz AP haben, erscheint das Fenster **Status von Drahtlosen Netzwerkverbindung**.
6. Klicken Sie auf **Eigenschaften**.
7. Die Dialogbox Eigenschaften von Drahtlosen Netzwerkverbindung erscheint.
8. Klicken Sie **Windows zum Konfigurieren der Einstellungen verwenden**, wählen Sie den Default Namen des von Ihrem Service Provider zur Verfügung gestellten APN.und klicken Sie **Konfigurieren**.
9. Achten Sie darauf, dass "Datenverschlusselüung (WEP aktiviert)", "Netzwerkauthentifizierung (gemeinsamer Modus)", und "Dies ist ein Computer-mit-Computernetzwerk (Ad-hoc); drahtlose Zugriffspunkte werden nicht verwendet" nicht ausgewählt sind und klicken Sie anschließend auf **OK**.
10. Der Default Name des von Ihrem Betreiber zur Verfügung gestellten APN erscheint nun im Bevorzugte Netzwerke Fenster.
11. Wählen Sie den Default Namen des von Ihrem Service Provider zur Verfügung gestellten APN und klicken Sie **Erweitert**.
12. Klicken Sie **Nur Zugriffspunktnetzwerke (Infrastruktur)** und klicken Sie **Schließen** .
13. Klicken Sie **OK**.

2: Konfigurieren Ihrer GPRS Karte

Um Ihre GPRS Karte für die Verbindung zu aktivieren, gehen Sie folgendermaßen vor:

1. Installieren Sie Ihre GPRS Karte entsprechend den Instruktionen des Herstellers.

2. Setzen Sie eine von Ihrem Mobilbetreiber zur Verfügung gestellte SIM Card in die GPRS Karte ein.

3. Setzen Sie die GPRS Karte in den PCMCIA Slot Ihres Notebooks.

4. Fahren Sie entweder fort mit "3: Automatisches Beziehen einer IP Adresse" falls zutreffend, oder mit "4: Download und Installation der SMART CLIENT Software".

Hinweis: *Wenn Sie Ihre WLAN Card zum Verbinden verwenden, können Sie die in den PCMCIA Slot des Notebooks eingesetzte GPRS Card als SIM Lesegerät anstelle des USB Kopierschutzschalters verwenden. Um dies zu tun, muss Ihr Notebook jedoch entweder zwei PCMCIA Slots haben (einen für die WLAN Card, einen für die GPRS Card), oder eine eingebaute WLAN Card und einen PCMCIA Slot.*

3: IP Adresse automatisch beziehen

Sie müssen diese Konfiguration nur durchführen, wenn Sie zuvor die Default-Einstellungen Ihrer WLAN Card geändert und Ihr Notebook zur Verwendung einer statischen IP-Adresse umkonfiguriert haben. Folgen Sie den Schritten "3.1 Konfiguration von DHCP und DNS für Windows 2000 und XP", um Ihr Notebook so zu konfigurieren, dass es eine IP Adresse automatisch über einen DHCP Server für Windows 2000 und Windows XP erhält.

3.1 Konfiguration von DHCP und DNS für Windows 2000 und XP

1. Für Windows 2000, wählen Sie **Startmenü>Einstellungen>Netzwerk- und DFÜ-Verbindungen.** Für Windows XP, klicken Sie mit der rechten Maustaste aus dem Startmenü **Netzwerkumgebung** und klicken Sie anschließend **Eigenschaften**.

2. Suchen Sie im Netzwerk-und DFÜ-Verbindungen Fenster Ihr **WLAN-Verbindung** Icon, klicken Sie darauf mit der rechten Maustaste und wählen Sie **Eigenschaften**.

3. Netzwerkverbindungen Fenster in Windows 2000.

4. Netzwerkverbindungen Fenster in Windows XP.

5. Das Eigenschaften von LAN Fenster erscheint.

6. Wählen Sie das **Internetprotokoll (TCP/IP)** und klicken Sie **Eigenschaften**.

7. Das Eigenschaften von Internetprotokoll (TCP/IP) Fenster erscheint.

8. Klick Sie auf die **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen**

9. Klicken Sie zweimal auf **OK**.

4: Download und Installation der SMART CLIENT Software

Folgen Sie den Schritten "4.1 Download und Installation der SMART CLIENT Software für Windows 2000 und Windows XP", um die SMART CLIENT Software für Windows 2000 oder Windows XP herunterzuladen und zu installieren.

4.1 Download und Installation der SMART CLIENT Software für Windows 2000 und Windows XP

Herunterladen und installieren der SMART CLIENT-Software

Bewegen Sie sich mit Ihrem eingeschaltetem Notebook in den Versorgungsbereich eines A1 WLAN HOTSPOTS und starten Sie den Browser. Ihr Browser wird automatisch auf die unten angeführte Begrüßungsseite umgeleitet:

> **Hinweis**: Falls die Begrüßungsseite Ihres Browsers leer sein sollte, geben Sie einen Domain-Namen ein (zum Beispiel *www.google.com*).

1. Klicken Sie auf den Hyperlink **Zum Herunterladen hier klicken**. Der Browser zeigt das Fenster **Datei zum Herunterladen** an.
2. Beim Internet Explorer, klicken Sie auf die Schaltfläche **Öffnen**. Bei Netscape, wählen Sie einen Ordner und klicken Sie auf **Speichern**. Ihr System beginnt mit dem Herunterladen der Datei und zeigt das Fenster mit der Sicherheitswarnung an. Klicken Sie auf ***Ja***, um fortzufahren.
3. Das Installationsfenster für den SMART CLIENT erscheint.
4. Klicken Sie auf die Schaltfläche **Weiter**. Jetzt erscheint das Fenster mit der Lizenzvereinbarung für den SMART CLIENT. Wenn Sie den Bestimmungen der Lizenzvereinbarung zustimmen, klicken Sie auf die Schaltfläche **Ich akzeptiere**. Daraufhin erscheint das Fenster **Installationsart auswählen**.
5. Wählen Sie **Standard**, um die SMART CLIENT-Software und den Treiber für den SIM-Reader zu installieren. Falls Sie den Treiber für den SIM-Reader (CardMan 6020) nicht installieren möchten, oder falls Sie das Verzeichnis ändern möchten, in dem die SMART CLIENT-Software oder der CardMan-Treiber installiert werden sollen, klicken Sie auf **Anpassen**.
6. Klicken Sie auf die Schaltfläche **Weite*r***. Jetzt erscheint das Fenster **Bereit zur Installation**.
7. Klicken Sie auf die Schaltfläche **Installieren**. Jetzt erscheint das Fenster **SMART CLIENT wird installiert**.
8. Wenn alle Dateien kopiert worden sind, steht die Schaltfläche **Weiter** wieder zur Verfügung. Klicken Sie auf die Schaltfläche **Weiter**. Jetzt erscheint das Fenster **Assistent für die Fertigstellung der Installation des SMART CLIENT** .
9. Klicken Sie auf die Schaltfläche **Beenden**. Der Assistent beendet die Installation und das Icon für den SMART CLIENT erscheint auf Ihrer Bildschirmarbeitsfläche.

10. Wenn der Assistent die Installation beendet hat, können Sie anhand des Piktogramms für den SMART CLIENT auf der Bildschirmarbeitsfläche erkennen, dass die Installation erfolgreich durchgeführt wurde.

5: Deinstallation der SMART CLIENT Software

Gehen Sie folgendermaßen vor, um den SMART CLIENT zu deinstallieren:

1. Trennen Sie Ihre Verbindung und schließen Sie die SMART CLIENT Applikation.
2. Schließen Sie die Konfigurations Utility der WLAN Karte, falls diese geöffnet ist.
3. Wählen Sie im Windows Toolbar Start > Einstellungen > Systemsteuerung > Software. Windows zeigt das Control Panel Fenster an.
4. Doppelklicken Sie auf das Hinzufügen/Entfernen von Programmen Icon.
5. Windows zeigt das Hinzufügen/Entfernen von Programmen Fenster an.
6. Wählen Sie A1 SMART CLIENT und klicken Sie auf Hinzufügen/Entfernen.
7. Windows zeigt das Möchten Sie das Programm wirklich entfernen Fenster an.
8. Klicken Sie ja. Windows entfernt den SMART CLIENT.

6: Neuinstallation der SMART CLIENT Software

Um die SMART CLIENT Software neu zu installieren, müssen Sie zuerst alle früheren SMART CLIENT Versionen vollständig entfernen. Um den SMART CLIENT neu zu installieren, führen Sie zuerst die Schritte aus, die in "5: Deinstallation der SMART CLIENT Software", beschrieben sind und anschließend die Schritte, die in "4: Download und Installation der SMART CLIENT Software" beschrieben sind.

Verwendung des A1 SMART CLIENT

Der SMART CLIENT arbeitet im Zusammenspiel mit dem CNP, um Ihnen Zugang zum Internet zu ermöglichen. Dieses Kapitel beschreibt den SMART CLIENT und seine Verwendung zur Verwaltung Ihrer Verbindung.

Kennenlernen des A1 SMART CLIENT

Mit Hilfe der SMART CLIENT Applikation können Sie die für Ihre Verbindung zum Internet über das Mobilkom Netz notwendigen Einstellungen vornehmen. Dieser Abschnitt stellt die verschiedenen Befehle und Einstellungen vor, die Sie festlegen und verändern können, um Ihre Internet Verbindung zu verwalten.

Um den SMART CLIENT zu starten, doppelklicken Sie auf das SMART CLIENT Icon auf Ihrem Desktop oder wählen Sie **Startmenu>Programme>A1 SMART CLIENT.**

Die Registerkarte Verbinden

Beim Öffnen des SMART CLIENT wird in der Grundeinstellung die Registerkarte Verbinden angezeigt.

Diese Aufstellung beschreibt die Funktion der Felder der Registerkarte.

Einstellung, Feld, oder Button	**Funktion**
Profil	Profile zeigt den Namen des Profils an, das gerade verwendet wird, um sich zu verbinden
Verfügebare Netzwerke	Zeigt eine Liste der Access Points (APs) innerhalb des Bereichs der WLAN Card Ihres Notebooks. Wenn Sie eine GPRS Card verwenden, zeigt das Fenster auch das verfügbare GPRS Netz an, für welches Ihre SIM Card berechtigt ist.
Signalstärke	Signalstärke gibt die Signalstärke jedes AP innerhalb der Reichweite der WLAN Card Ihres Notebooks an
Netzsuche Button	Klicken Sie auf diesen Button, um eine Suche nach verfügbaren APs innerhalb der Reichweite der WLAN Card Ihres Notebooks zu starten
Verbinden/Trennung button	Wenn keine Verbindung zu einem AP besteht, löst das Klicken des **Verbinden** Button den Verbindungsvorgang zum gewählten AP aus. Wenn eine Verbindung zu einem AP besteht, wird durch Klicken auf den **Trennung** Button der Trennvorgang ausgelöst.

Verbindungsinfo	Zeigt Details über die aktuelle Verbindung an • Name (SSID oder GPRS Netz)—der Service Set Identifier Name (SSID) des AP oder der Name des GPRS Netzes, zu dem Sie verbunden sind • Signalstärke—ist ein Maß für die relative Amplitude des Signals zwischen dem AP und der WLAN Card Ihres Notebooks • Verbindungsqualität—ist ein Maß für die Anzahl der verlorenen Pakete und Datenfehler • Aktivität—gibt die Anzahl der TCP/IP Pakete an, die zwischen der WLAN Card Ihres Notebooks und dem AP oder GPRS Netz gesendet werden • Verbindungzeit—gibt die Dauer der aktuellen Verbindung an

Hinweis: *Durch Klicken auf den Trennung Button bei bestehender Verbindungwird der SMART CLIENT minimalisiert. Wenn der Trennung Button geklickt wird, ohne dass eine Netzwerkverbindung besteht, dann wird der SMART CLIENT dadurch geschlossen.*

Die Registerkarte Konfigurieren

Die Registerkarte Konfigurieren können Sie verwenden, um Benutzerprofile zum Einloggen mit vordefinierten Konfigurationseinstelllungen anzulegen, zu kopieren und zu ändern..

Ein Profil ermöglicht es Ihnen, die Wireless LAN Einstellungen zu konfigurieren und einen Access Point für die Verbindung zum CNP vorzuselektieren, und auch Mobilnetzeinstellungen für Authentifizierung und Verschlüsselung zu konfigurieren.

Die Registerkarte Info

Die Registerkarte Info zeigt Informationen über den SMART CLIENT an, wie z.B. die Versionsnummer und das Copyright Datum.

1: Anlegen eines neuen Profile

Sie können entweder die Default-Profileinstellungen im SMART CLIENT verwenden oder eines oder mehrere persönliche Profile anlegen. Das Anlegen eines Profils ermöglicht es Ihnen, vordefinierte Konfigurationsparameter abzuspeichern, die für verschieden Standorte und Umgebungen optimiert sind. Wenn Sie ein Profil abgespeichert haben, können Sie jedes Mal, wenn Sie von einem Standort und/oder einer Umgebung, die einem Ihrer Profile entspricht, eine Verbindung zum A1 WLAN - Netzwerk herstellen möchten, einfach das entsprechende Profil aus der Auswahlliste im Abschnitt **Profile** der Registerkarte **Konfigurieren** oder durch Klicken auf die Schaltfläche **Konfiguration auswählen** unter der Registerkarte **Verbinden auswählen**.

Zum Anlegen eines neuen Profils:

1. Starten Sie den SMART CLIENT und klicken Sie auf die Registerkarte Konfigurieren.
2. Klicken Sie auf die Schaltfläche Neu im Abschnitt Profil der Registerkarte Konfigurieren„Neues Profil" erscheint im Feld Wählen Sie das Profil, das Ihre Einstellungen enthält.
3. Geben Sie den Namen des neuen Profils ein und klicken Sie WeiterWeiter.
4. Das Profile Type Fenster erscheint.
5. Wählen Sie entweder die **Zu-Hause Profil** oder **Mobil Profil** Optionen, je nachdem, welche Art von Verbindungsprofil Sie anlegen wollen, dann klicken Sie **Weiter**.

Wenn Sie zu-hause profil wählen, fahren Sie mit dem Unterpunkt 1.1 fort.

Wenn Sie mobil profil wählen, fahren Sie mit dem Unterpunkt 1.2 fort.

1.1 Anlegen eines Profils für ein Heim Netz

Das Access Point Auswahlfenster erscheint.

1. Wählen Sie entweder **Verwendung eines bestimmten Zugangspunktes** oder **Verwendung eines beliebigen Zugangspunktes**.
2. Bei **Verwendung eines bestimmten Zugangspunktes**, wird das Name des **Zugangspunktes** Feld editierbar. Geben Sie die **SSID** Ihres Zugangspunktes In diesem Feld ein. Klicken Sie **Weiter**.
3. Das Central AP oder Peer-to-Peer Fenster erscheint.
4. Wenn Sie einen AP verwenden (entweder einen spezifischen AP oder irgendeinen verfügbaren AP), klicken Sie auf die Check Box neben Ich verfüge über einen Zugangspunkt.
5. Wenn Sie ein Peer-to-Peer Netz verwenden, lassen Sie die Box ohne Häkchen. Klicken Sie **Weiter**
6. Das WEP-Verschlüsselung Fenster erscheint.
7. Wenn der AP, zu dem Sie sich verbinden wollen, WEP Verschlüsselung aktiviert hat, müssen Sie auf die **WEP-Verschlüsselung freigeben** Check Box klicken.
8. Wenn der AP, zu dem Sie sich verbinden wollen, WEP Verschlüsselung nicht aktiviert hat, lassen Sie diese Box ohne Häkchen.

Hinweis: *Mobilkom empfiehlt, die WEP Verschlüsselung bei Verbindungen zu Ihrem Heimnetz AP zu aktivieren. Wenn Sie sich jedoch zu A1 WLAN verbinden, bieten die Standard-Sicherheits Features des SMART CLIENT einen bedeutend besseren Schutz für Ihren wireless LAN als die WEP Verschlüsselung.*

Klicken Sie **Weiter**.

9. Wenn Sie Enable WEP Encryption ausgewählt haben, erscheint das WEP Keys Fenster.

10. Wählen Sie entweder 128 bit oder 40 bit encryption strength aus.

11. Geben Sie WEP Verschlüsselungs-Keys in eines oder mehrere der vier Felder ein, wählen Sie den gewünschten **Verwendeter Schlüssel** (1-4), und klicken Sie **Weiter**.

Hinweis: *Sie müssen die WEP Verschlüsselungs Keys von der Konfigurations Utility Ihres APs erhalten. Details über das Spezifizieren und Konfigurieren der WEP Keys entnehmen Sie bitte der Dokumentation des Herstellers Ihres APs.*

Das Profil Complete Fenster erscheint.

Klicken Sie auf **Finish**.

Sie kehren zurück zur Registerkarte Konfigurieren Ihres SMART CLIENT, welche jetzt den Namen des Profils zeigt, das Sie gerade in der **Redigieren Sie Profil-Einstellungen** Liste angelegt haben.

1.2 Anlegen eines Profils für ein Mobilnetz

Das Access Point Auswahlfenster erscheint.

1. Wählen Sie entweder **Vervendung eines bestimmten Zugangspunktes** oder **Verwendung eines beliebigen Zugangspunktes**.

2. Bei **Verwendung eines bestimmten Zugangspunktes**, wird das Name des **Zugangspunktes** Feld editierbar. Geben Sie die **SSID** Ihres Zugangspunktes In diesem Feld ein.

3. Klicken Sie **Weiter**.

4. Das Authentifizierungsfenster erscheint.

5. Wählen Sie **SIM-Karte** oder **Benutzerkennung und Passwort**, und klicken Sie **Weiter**.

6. Bei Auswahl von **SIM-Karte** fahren Sie mit Schritt 3 fort.

7. Bei Auswahl von **Benutzerkennung und Passwort** springen Sie weiter

8. Das Access Point Name (APN) Informationsfenster erscheint.

9. Wenn Sie von Ihrem Mobilbetreiber APN Information erhalten haben, klicken Sie auf die **Ich kenne den APN** Check Box.

Hinweis: *Zusätzlich zur Authentifizierungsinformation auf Ihrer SIM Karte, verlangen manche Betreiber eine zweite Stufe der Authentifizierung mit Benutzerkennung und Passwort. Dadurch sollen unberechtigte Zugriffe auf Ihren Account im Fall einer gestohlenen SIM Karte verhindert werden.*

Wenn Sie auf die Check Box **Ich kenne den APN** klicken, erscheint das APN Konfigurationsfenster..

10. Klicken Sie auf **Anmeldung erforderlich** und geben Sie den Domain Name für Ihren Mobil-Servicebetreiber im **APN** Feld ein: A1.net

Die folgenden Schritte sind optional. Sie ermöglichen Ihnen, den Login Usernamen und das Passwort für Ihren Mobilnetz Account zu spezifizieren. Wenn Sie diese Parameter oder einen von Ihnen bei der Authentifikation zum CNP über Ihre SIM Karte im SMART CLIENT angeben, leitet der CNP Ihre Login-Information automatisch an Ihren Mobil-Service Provider weiter.

Geben Sie im Feld **Benutzername** Ihren Mobilnetz Login-Namen ein.

Klicken Sie auf **Erinnerung an mein Passwort** und geben Sie das Login Passwort für Ihren Mobilnetz Account ein, klicken Sie anschließend **Weiter**.

Hinweis: *Wenn Sie Erinnerung an mein Passwort nicht anklicken und Ihr Passwort eingeben, werden Sie bei jeder Authentifizierung zum CNP nach Ihrem Mobilnetz Passwort gefragt. Wenn Sie Ihren Benutzernamen nicht angeben, werden Sie bei jeder Authentifizierung nach Ihrem Benutzernamen und Ihrem Passwort gefragt.*

Das Profil Complete Fenster erscheint.

Klicken Sie **Finish**.

Sie kehren zurück zur Registerkarte Konfigurieren Ihres SMART CLIENT, welche jetzt den Namen des Profils zeigt, das Sie gerade in der Redigieren Sie Profil-Einstellungen Liste angelegt haben.

2: Editieren eines bestehenden Profils

Wenn Sie einmal ein Verbindungs-Profil angelegt haben, können Sie alle im Profile Wizard spezifizierten Parameter verändern. Sie können auch Default-Parameter verändern, welche Sie im Profile Wizard nicht ändern oder auswählen können.

Beim Editieren eines bestehenden Profils können Sie folgende Änderungen vornehmen:

• Ändern des Profilnamens

• Ändern der Access Point Auswahlkriterien

• Ändern des Wireless LAN Mode (Infrastructure oder Adhoc)

• Aktivieren oder Deaktivieren der WEP Verschlüsselung

• Verändern der Authentifizierungsparameter

• Verändern der Default Timeout Werte

• Aktivieren/Deaktivieren des Loggings von Verbindungsversuchen und Angabe des Speicherortes der Log Files.

Gehen Sie folgendermaßen vor, um ein bestehendes Profil zu editieren:

1. Starten Sie den SMART CLIENT und klicken Sie auf die Registerkarte Konfigurieren.
2. Wählen Sie das Profil, das verändert werden soll in der Redigieren Sie Profil-Einstellungen Liste und klicken Sie Edit. Das Profil-Editor für A1 SMART CLIENT Fenster erscheint.

Die Konfigurationseinstellungen sind unter drei Überschriften gruppiert:

• Einstellungen

— Profilname

— Access Point Auswahl

• WLAN Einstellungen

— Modus

— WEP-Verschlüsselung

• Mobile Netzeinstellungen

— Authentifizierung

— Time out

— Protokollierung

Öffnen Sie die Überschrift Einstellungen und klicken Sie auf Profilname.

Das Profilname Feld erscheint.

3. Geben Sie den neuen Profilnamen ein.
4. Klicken Sie auf Access Point Auswahl.
5. Das Access Point Feld erscheint.
6. Wählen Sie im SSID Feld einen der verfügbaren APs oder wählen Sie später wählen.
7. Öffnen Sie die Wireless LAN Settings Überschrift und klicken Sie auf Modus.

Das WiFi-Netzwerktyp Feld erscheint.

8. Wählen Sie infrastruktur oder adhoc im Typ Feld.
9. Klicken Sie auf WEP-Verschlüsselung.

Das WEP-Verschlüsselung Feld erscheint.

10. Wenn Sie WEP Verschlüsselung aktivieren, wählen Sie die Verschlüsselungsstärke, 40 Bit oder 128 Bit und geben Sie einen oder mehrere WEP Schlussel ein, wie es unter Aufgabe "1.1Anlegen eines Profils für ein Heim Netz" weiter oben beschrieben ist.

11. Öffnen Sie die Überschrift Mobile Network Settings und klicken Sie auf Authentication.

Das Netzwerk-Authentifizierung Feld erscheint.

12. Wählen Sie eine der folgenden Authentifizierungsoptionen:

— SIM

— SSL SIM

Falls nötig, können Sie die APN Information eingeben oder editieren, wie es in Aufgabe "1.2Anlegen eines Profils für ein Mobilnetz", weiter oben beschrieben ist.

13. Click Timeouts.

Das Time Out Feld erscheint.

14. Bewegen Sie den Schieber nach links, um den Timeout Interval zu verkleinern und nach rechts, um den Timeout Interval zu vergrößern oder klicken Sie Restore Default um zur Standardeinstellung Einstellung des SMART CLIENT zurückzukehren.

15. Click **Logging**.

Das Protokollierung Feld erscheint.

16. 16 TUm das Protokollieren von Verbindungsversuchen zu aktivieren, klicken Sie auf Verbindungsprotokollierung.

17. Um den Speicherplatz des Log Files anzugeben, klicken Sie auf Protokolldatei auswälen. Navigieren Sie nach dem Öffnen der Dialog Box zum Verzeichnis, in dem Sie das Log File speichern wollen, und klicken Sie Open.

18. Klicken Sie auf OK, um Ihre Änderungen zu speichern und anzuwenden.

Sie gelangen zurück zur Registerkarte Configure des SMART CLIENT. Die von Ihnen geänderten Einstellungen kommen bei Ihrer nächsten Verbindung zu einem CNP mit dem geänderten Profil zur Anwendung.

Verbindung zum Internet

Gehen Sie folgendermaßen vor, um sich mit dem SMART CLIENT zum Internet zu verbinden:

1. Starten Sie den Mobilkom SMART CLIENT durch Doppelklick auf sein Icon am Desktop oder durch Auswahl von **Startmenü>Programme>A1 SMART CLIENT**

2. Wählen Sie das Profil, das Sie für diese Verbindung verwenden wollen. Wenn Sie kein Profil angelegt haben, verwenden Sie Default.

3. Klicken Sie auf **Netzsuche**.

Wenn die Suche abgeschlossen ist, sollten Sie wenigstens einen CNP AP sehen.

4. Wählen Sie einen CNP AP aus und klicken Sie auf Verbinden.

Ein Verbindungsstatus-Fenster erscheint, welches den Verlauf der Verbindungsherstellung anzeigt..

> Hinweis: *Wenn die Signalstärke des AP, zu dem Sie sich verbinden wollen,schwach ist, sollten Sie sich näher darauf zubewegen und nochmals versuchen, die Verbindung herzustellen.*

Wenn die Verbindung hergestellt wurde, erscheint der AP Name im Verbindungsinfo Abschnitt der Registerkarte Verbinen, wo **Signalstärke** und **Verbindungsqualität** der Verbindung angezeigt werden.

Trennen der Internet-Verbindung

Gehen Sie folgendermaßen vor, um die Verbindung zum Internet zu trennen:

1. Klicken Sie **Trennung** in der Registerkarte Verbinden.

Der SMART CLIENT zeigt das **Trennen der Verdindung** Popup und stellt den Verlauf der Trennung durch Meldungen in der Status Zeile dar, wie unten gezeigt.

Troubleshooting

Dieses Kapitel liefert Informationen über häufige Fehler und deren Behebung.

Häufige Fehler und deren Behebung

Ich habe keine Verbindung, aber mein SIM Karte Leser blinkt rot.

Der SIM Karte Leser kann Ihre SIM Karte nicht lesen. Vergewissern Sie sich,dass die Goldkontakte auf der Unterseite der Karte nach unten weisen und dass sie auf die Kontakte des Lesers ausgerichtet sind. Sie sind nicht richtig ausgerichtet,wenn Sie Ihre SIM Karte verkehrt in den Leser stecken.

Die Lichter auf meinem SIM Karte-Leser leuchten nicht.

Ihr Notebook kann nicht mit Ihrer SIM Karte kommunizieren. Überprüfen Sie die Verbindung zwischen dem USB und der SIM Card. Überprüfen Sie, ob Sie den USB Port benutzen, auf den Sie den SIM Karte Treiber konfiguriert haben.

Meine SIM Karte scheint mit dem Notebook zu kommunizieren, aber ich kann keine Berechtigung für eine Verbindung zum CNP erhalten.

Ihre SIM Karte wurde möglicherweise nicht ordnungsgemäß freigeschalten. Kontaktieren Sie Ihren Mobilbetreiber.

Nach dem Anklicken des Default Access Point erhalte ich folgende Meldung: "Unable to select <Name_of_AP>".

Diese Meldung kann verschieden Ursachen haben. Gehen Sie folgendermaßen vor, um das Problem einzugrenzen:

Starten Sie das Utility Programm für Ihre WLAN Karte. Wenn die Werte für Verbindungsqualität und Signalstärke 0 sind, oder wenn die Utility anzeigt, dass die Karte Nicht verbunden ist, prüfen Sie die Lichter auf Ihrer Karte. Wenn sie nicht leuchten, kommuniziert Ihre Karte nicht mit Ihrem Notebook. Stellen Sie sicher, dass sie korrekt in ihrem Einschubplatz sitzt. Wenn die Karte mit Ihrem Notebook kommuniziert, könnte der AP gestört sein.

Wenn das Utility Programm anzeigt, dass Sie eine Verbindung zum AP haben, überprüfen Sie, ob sich die Karte auf der Liste der unterstützten Karten befindet. Wenn das nicht der Fall ist, kontaktieren Sie Ihren Netzadministrator, damit er Ihre Karte gegen eine unterstützte austauscht.

Wenn sich Ihre Karte auf der Liste der unterstützten Karten befindet, benachrichtigen Sie Ihren Netzadministrator, damit er das Problem weiter eingrenzen kann.

Mein Computer verbindet sich zu einem AP, aber nachdem ich die WLAN Karte austausche, kann ich mich nicht zum Default CNP AP verbinden.

Stoppen Sie den SMART CLIENT und starten Sie ihn neu. Eine Verbindung sollte jetzt möglich sein.

Auf dem Notebook ist ein fremdes VPN Programm installiert. Nach der Installation des SMART CLIENT verlor ich die Verbindung zum Netzwerk.

SMART CLIENT besitzt einen Netzfilter-Treiber, der den Netzwerkverkehr steuert. Wenn ein Fremdprogramm auch einen Filter-Treiber besitzt, können die beiden Treiber einander beeinflussen. Der SMART CLIENT muss vor der VPN Software installiert werden. Zur Beseitigung des Problems deinstallieren Sie das VPN Programm, installieren Sie den SMART CLIENT und installieren Sie anschließend wieder das VPN.

Meine Hardware ist korrekt konfiguriert, die Treiber sind installiert, aber ich kann keine Verbindung herstellen.

Überprüfen Sie, ob Sie andere Kommunikationseinrichtungen haben, die mit Ihrer WLAN Card in Konflikt geraten können. Sollte dies der Fall sein, deaktivieren Sie dieses Gerät und entfernen Sie seinen Treiber. Details finden Sie in der Windows Dokumentation.Es kann auch notwendig sein, dass Sie Ihren WLAN Card-Treiber entfernen und neu installieren. Achten Sie auch darauf, dass die Konfigurations-Utility für Ihre Karte installiert ist. Rufen Sie sie auf und stellen Sie auf ihrer Konfigurationsseite den Mode Ihrer Karte auf Infrastructure.

Überprüfen Sie den Status Ihrer Verbindung durch das Absetzen des folgenden Befehls von einem DOS Fenster: ipconfig/all. Die Karte sollte eine IP Adresse ohne Null haben. Wenn das nicht der Fall ist, verwenden Sie den Befehl ipconfig/renew. Wenn Sie dadurch keine IP-Adresse für die Karte erhalten, rebooten Sie Ihr System.

Ich habe gerade die SMART CLIENT Software installiert, aber mein Notebook kann nicht mit dem SIM Lesegerät kommunizieren.

Überprüfen Sie, ob der SIM-Leser in seinem Einschub ordnungsgemäß sitzt.

Wenn Sie den SMART CLIENT zum ersten Mal installieren, warten Sie ca. 15 bis 30 Sekunden nach dem Klicken des Finish Button, um abzuwarten, bis Windows mit dem Konfigurieren des Treibers des SIM Lesers im Hintergrund fertig ist.

Glossar

AES	Advanced Encryption Standard—ein Verschlüsselungsalgorithmus für die Sicherung von heiklem, aber nicht geheimem Material durch die Regierung der USA, welcher mit großer Wahrscheinlichkeit letztendlich zum de facto Verschlüsselungsstandard für kommerzielle Transaktionen auf dem privaten Sektor werden wird. Die AES Spezifikation verwendet einen symmetrischen Algorithmus (derselbe Schlüssel für Verschlüsselung und Entschlüsselung) mit Block-Verschlüsselung von 128 Bits Größe, welche die Schlüsselgrößen von 128, 192 und 256 Bits als Minimum unterstützen.
AP	Access Point
CNP	Converged Network Platform
DHCP	Dynamic Host Configuration Protocol—ein Kommunikationsprotokoll, das es Netzadministratoren ermöglicht, die Zuweisung von Internet Protocol (IP) Adressen im Netzwerk einer Organisation zentral und automatisiert zu verwalten.
DNS	DNS Domain Name System—die Methode, mit der Internet Domänen Namen gefunden und in Internet Protocol Adressen übersetzt werden. Ein Domänen Name ist eine aussagekräftige und leicht zu merkende "Bezeichnung" für eine Internet Adresse. Da es unpraktisch wäre, eine zentrale Liste von Domänennamen/IP-Adressen-Zuordnungen zu verwalten, werden die Listen der Domänennamen und IP Adressen über das Internet in einer Autoritätshierarchie verteilt. DNS Server mappen die Domänennamen in Internet Anforderungen auf spezifische IP Adressen oder leiten sie an andere Server im Internet weiter, die dieses Mapping vornehmen können.
GGSN	Gateway GPRS Support Node—die Schnittstelle zwischen dem GPRS Backbone Netzwerk und den externen Paketdaten-Netzwerken. Sie konvertiert die vom SGSN Kommenden GPRS Pakete in das richtige Paketdatenprotokoll (PDP)-Format (z.B., IP oder X.25) und versendet sie auf dem entsprechenden Paketdaten-Netzwerk. In deranderen Richtung werden PDP Adressen von kommenden Datenpaketen zur GSM Adresse des empfangenden Benutzers konvertiert.
GPRS	General Packet Radio Service—ein paketbasierendes Mobilkommunikationsservice mit Datenraten von 56 bis zu 114 Kbps und ununterbrochener Verbindung zum Internet für Benutzer von Mobiltelephonen und–computern.
GSN	GPRS Support Node—eine GPRS Netzwerkkomponente, die für die Zustellung der Datenpakete zwischen den Mobiltelefonen und den externen Paketdatennetzen (PDN) zuständig ist.
GTP	GPRS Tunneling Protocol—ein Protokoll, welches die Kommunikation der Support Nodes in einem GPRS Netz untereinander ermöglicht.

GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol—die Gesamtheit an Regeln für den Austausch von Files (Text, Grafiken, Sound, Video, und andere Multimedia Files) im World Wide Web. HTTP ist ein von der TCP/IP Protokollfolge (welche die Basis für Informationsaustausch im Internet darstellt), abhängiges Applikationsprotokoll.
ID	Identifier
IP	Internet Protocol—das Protokoll, unter dem Daten von einem Computer zu einem anderen im Internet gesendet werden. Jeder Computer im Internet hat zumindest eine IP Adresse, die ihn eindeutig gegenüber allen anderen identifiziert. Wenn Sie Daten senden oder empfangen (zum Beispiel Email oder eine Web-Seite), wird die Nachricht in Pakete aufgeteilt. Jedes Paket enthält die Internet Adresse des Absenders und des Empfängers. Jedes Paket wird zuerst an einen Gateway Computer gesendet, der einen kleinen Teil des Internet versteht. Der Gateway Computer liest die Zieladresseund leitet das Paket an einen benachbarten Gateway weiter, der wiederum die Zieladresse liest und so weiter durch das Internet, bis ein Gateway erkennt, dass das Paket zu einem Computer in seiner unmittelbaren Umgebung oder Domäne gehört. Der Gateway sendet dann das Paket direkt an den Computer mit der angegebenen Adresse.
OMC	Operations & Maintenance Center
PPP	Point-to-Point Protocol—ein Protokoll für die Kommunikation zwischen zwei Computern mittels serieller Schnittstelle, typischerweise eines PCs, der über eine Telefonleitung an einen Server angeschlossen ist.
SIM	Subscriber Identity Module—zum Einschieben in ein Mobiltelefon. Diese SIM oder "smart" card Enthält alle teilnehmerbezogenen Daten, wie Telefonnummern, Service Details und Speicherplatz für Nachrichten. Mit einer SIM Card können Anrufe von jedem zulässigen Mobiltelefon aus gemacht werden, da die Teilnehmerdaten –nicht die interne Seriennummer des Telefons –für den Anruf verwendet werden.
SSL	Secure Socket Layer—ein allgemein verwendetes Protokoll für das Management der Security Einer Nachrichtenübertragung im Internet. SSL würde kürzlich von Transport Layer Security (TLS), abgelöst, welches auf SSL basiert. SSL verwendet eine Programmschicht, die sich zwischen der Hypertext Transfer Protocol (HTTP) Schicht des Internet und der Transport Control Protocol (TCP) Schicht befindet. SSL ist ein Teil sowohl des Microsoft und des Netscape Browsers und der meisten Web Server Produkte. SSL, welches von Netscape entwickelt wurde, erhielt auch die Unterstützung von Microsoft und anderer Internet Client/Server Entwickler und wurde zum de facto Standard bis es sich in Transport Layer Security weiter entwickelte. Der "sockets" (Anschlussbuchsen) Teil des Namens nimmt Bezug auf die Methode, Daten zwischen einem Client und einem Server Programm in einem Netzwerk oder zwischen Programmschichten in demselben Computer hin- und herzusenden. SSL verwendet das öffentlich-und-private Verschlüsselungssystem von RSA, welches auch die Verwendung eines digitalen Zertifikats einschließt.
USB	Universal Serial Bus

VPN	Virtual Private Network—eine Methode zur Nutzung einer öffentlichen Telekommunikations-Infrastruktur, wie z.B. Internet, um örtlich entfernten Niederlassungen oder Einzelteilnehmern einen sicheren Zugang zum Netz ihrer Organisation zu ermöglichen. Ein VPN kann einem teuren System von Stand- oder Mietleitungen gegenübergestellt werden, die nur von einer Organisation verwendet werden können. Das Ziel eines VPN ist es, der Organisation dieselben Möglichkeiten zu bieten, aber zu wesentlich niedrigeren Kosten. Ein VPN funktioniert durch Verwendung der gemeinsamen öffentlichen Infrastruktur bei gleichzeitiger Wahrung der Datensicherheit durch Sicherheitsmethoden und Tunnelungsprotokolle, wie z.B. das Layer Two Tunneling Protocol (L2TP). Indem sie die Daten beim Sender verschlüsseln und beim Empfänger entschlüsseln, senden diese Protokolle die Daten tatsächlich durch einen "Tunnel", der von nicht richtig verschlüsselten Daten nicht "betreten" werden kann. Eine zusätzliche Sicherheitsstufe wird dadurch erreicht, dass nicht nur die Daten, sondern auch die sendende und die empfangende Netzwerkadresse verschlüsselt werden.
WEP	Wired Equivalent Privacy—ein Sicherheitsprotokoll für wireless local area (WLANs), welches im Standard 802.11b definiert ist. WEP wurde entwickelt, um dasselbe Maß an Sicherheit zu bieten, wie in einem Festnetz-LAN. LANs sind von Natur aus sicherer als WLANs, da sie durch die physikalischen Gegebenheiten geschützt sind, indem sich ihre gesamte Netzwerkstruktur oder der Großteil davon innerhalb eines Gebäudes befindet, welches gegen unberechtigte Zugriffe geschützt werden kann. WLANs, welche über Funkwellen realisiert werden, haben nicht dieselbe physikalische Struktur und sind daher anfälliger für Missbrauch. WEP hat das Ziel, Sicherheit zu bieten, indem die Daten über Funkwellen verschlüsselt werden, sodass sie bei der Übertragung geschützt sind. Es stellte sich jedoch heraus, dass WEP nicht so sicher ist, wie man einmal angenommen hat. WEP wird in den zwei untersten Schichten des OSI Modells verwendet – den Datenverbindungs- und physikalischen Schichten; daher bietet es keine End-to-End Sicherheit.
WLAN	Wireless Local Area Network
WSC	Wireless Services Gateway