1. Motivation

Ausgangspunkt für EMVA ist die Beobachtung, dass die Resource PKW insbesondere bei täglichen Fahrten zum Arbeitsort und zurück („Pendler“) gemessen an seiner Personen-Aufnahmekapazität im Schnitt zu weniger als 50% ausgelastet ist. Diese „Resourcen-Verschwendung“ wird durch kontinuierlich steigende Nebenkosten (für Treibstoff, Steuern etc.) zunehmend unattraktiv. Gleichzeitig gibt es für Bewohner außerhalb von Ballungszentren oftmals aber keine praktische Alternative in Form von öffentlichen Verkehrsmitteln.

Mit Hilfe eines neuen Geschäftsmodells („Adhoc-Mitfahr-Vermittlung“) und neuen technischen Möglichkeiten drahtloser Kommunikation kann EMVA sowohl die Resourcen-Auslastung der Fahrzeuge steigern mit damit verbundenen finanziellen Vorteilen für den einzelnen Pendler wie auch einen sinnvollen Beitrag zur Umweltschonung leisten.

2. Geschäftsmodell

Die Grundidee für EMVA ist es, das bekannte „Trampen“ auf eine neue Basis zu stellen, indem es den Teilnehmern (Fahrer/Mitfahrer) folgende Vorteile bietet:

- **Sicherheit**
  wird gewährleistet durch Maßnahmen des EMVA-Betreibers wie
  - Registrierung der Teilnehmer
  - Vorlage eines polizeilichen Führungszeugnisses
  - Auszug aus Flensburg-Register für den Faher
  - Verwendung fälschungssicherer Ausweise (SmartCard) zur Authorisierung
  - Gewährleistung eines sicheren, bequemen und transparenten Abrechungsverfahrens.
  - weitere durch die Benutzer konfigurierbare Sicherheitsmerkmale denkbar, wie z.B. „nur Mitfahrerinnen“ bzw. „nur Fahrerinnen“ oder Alterseinschränkungen, Fahrzeugmerkmale etc.
- **Einnahmen für den Fahrer**
  Der Fahrer kann durch die Mitnahme eines oder mehrerer Fahrgäste seine Fahrtkosten zum Teil oder ganz decken. Die anfallenden Registrierungskosten für den Erhalt eines fälschungssicheren Ausweises für den Fahrer armortisieren sich in kurzer Zeit (wenige Wochen).
- **Kostenersparnis für den Mitfahrer**
  Der Mitfahrer spart sich die Kosten für Treibstoff und Abnutzung. Eventuell kann er hierdurch zur Gänze auf ein Fahrzeug verzichten. Die anfallenden Registrierungskosten für den Erhalt eines fälschungssicheren Ausweises armortisieren sich in kurzer Zeit (wenige Wochen). Die Kosten für die Mitfahrten sind attraktiv niedrig.
- **Einfachheit**
  die Benutzung des Systems ist nicht komplizierter als eine SMS per Handy zu schicken.
- **soziale Attraktivität**
  ein weiterer Vorteil kann darin liegen, neue Menschen kennen zu lernen oder sich während der Fahrt angenehm unterhalten zu können.
- **technischer Touch**
  diesen Aspekt sollte man im „SMS-Zeitalter“ nicht unterschätzen. Auch der Erfolg des „Mountain-Bikes“ welches das Fahrrad auf eine gewisse Art neu erfand, kann hier angeführt werden. „Mobile Computing“ ist Hype!
- **Hardware-Verbreitung**
  Der Marktanteil von Windows Mobile Geräten steigt kontinuierlich und wird wegen der Dominanz von Microsoft zweifellos Palm-basierte Geräte über kurz oder lang verdrängen. Zudem sind die Entwicklungswerkzeuge für Windows Mobile Geräte wesentlich professionieller und ausgereifter als bei Palm.
- **schnelle Marktdurchdringung**
  EMVA muss sehr schnell einen hohen Marktanteil erobern, da das Verfahren ziemlich leicht nachgebaut werden könnte. Um dieses Ziel zu erreichen, wird auch auf die Einführung einer propriätären Hardwarelösung verzichtet. Stattdessen sollen als Zielplattform Pocket PC’s mit Windows Mobile 2003 SE oder höher mit integrierter WLAN Karte dienen.

Der Gewinn für EMVA liegt darin, bei der Abwicklung des eigentlichen Zahlungsvorganges eine prozentuale Gebühr zu erheben (5-10%). Das entspricht in etwa dem Modell, wie ebay funktioniert.

3. Verfahrens-Beschreibung

3.1 Voraussetzungen

- alle Teilnehmer sind beim EMVA-Betreiber registriert und verfügen über einen geeigneten Pocket PC (PPC) mit WLAN für die drahtlose Kommunikation und Steckplätzen für Speicherkarte und Anschlußmöglichkeit für SmartCard-Reader
- die WLAN-Karten der Pocket PC's kommunizieren im sog. ad-hoc Modus, bei dem kein externer Access Point wie etwa bei Hotspots in Hotels oder Flughäfen nötig ist, d.h. die Kommunikation erfolgt autark. Die Netzwerk-Einstellungen bis zur IP-Adresse sind vom Betreiber vorgegeben und sollen möglichst automatisch eingestellt werden (dabei sind evtl. Konfigurationsprofile zu verwalten!).
- die PPC's empfangen bzw. senden Daten i.W. nur „von vorne" bzw. „nach vorne". Damit ist gewährleistet, dass keine unnötige Kommunikation entsteht, indem z.B. ein Fahrzeug auf der Gegenfahrbahn kontaktiert wird.
- persönliche und nicht veränderliche Daten (z.B. Bild, Schlüsselbund, Ident-Nr.) sind auf einer SmartCard abgelegt. Diese ist gegen Manipulationen von außen und vor unberechtigtem Zugriff mit einer PIN geschützt
- sensible Daten werden stets verschlüsselt übertragen.

3.2 Ablauf

Die folgenden Schritte beschreiben ein Standard-Szenario für einen typischen Geschäftsvorfall.

1. Der Fahrer (im folgenden EMVA-Server genannt) schaltet den PPC an und meldet sich mit der SmartCard und einer PIN am System an. Dabei wird auch überprüft, ob auf der eingelegten Speicherkarte gnügend Platz frei ist (für Kontierungsdaten).

2. Für den EMVA-Server sind bezogen auf die Orte, die von einem EMVA-Client angefragt werden können, Positiv- oder Negativlisten einstellbar. Damit wird erreicht, dass vom EMVA-Client erzeugte Anfragen gezielt gefiltert werden können.
   Denkbar ist auch die Verwendung von Platzhalterzeichen (z.B. Jokerzeichen ‚?' und ‚*') und die Angabe von Postleitzahlbereichen. Für die Positivliste ist einstellbar, ob ausschließlich Anfragen aus dieser Liste angezeigt werden sollen oder ob Anfragen aus der Positivliste nur priorisiert werden (evtl. farbliche Markierung und Signalton).

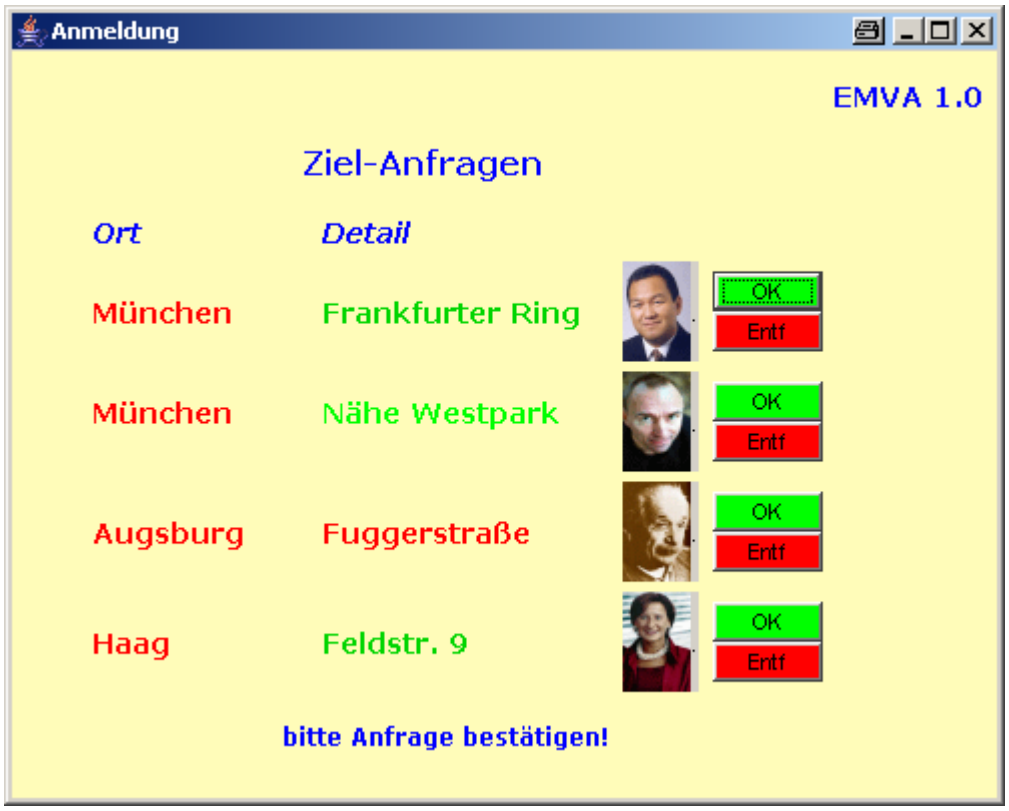
3. Für einen EMVA-Client verläuft die Anmeldung an seinem PPC analog wie oben beschrieben. Er trägt das Fahrtziel in zwei Felder Grobziel (z.B. Stadt) sowie Feinziel (z.B. Strasse, Ortsteil) ein. Weitere Wunschmerkmale wie Fahrzeugtyp (siehe oben unter Sicherheit) sind in einer Profil-Datei gespeichert. Für das Feld Feinziel sind zwei Varianten ‚mandatory' und ‚optional' vorgesehen, je nachdem ob dieses vom EMVA-Server zwingend anzufahren ist oder nicht. Dabei sind Mischformen denkbar, z.B. (Grobziel='München', Feinziel='Osten', Variante='mandatory'). Die beiden Varianten (optional ja oder nein) werden im Display des EMVA-Servers bei einer Anfrage in unterschiedlichen Farben (rot/grün) dargestellt.

4. Der EMVA-Client PPC sucht auf Knopfdruck oder kontinuierlich (einstellbar) in der Richtung, in welches es gehalten wird über zyklische ICMP Broadcast-Nachrichten (oder Multicast) einen möglichen EMVA-Server.

5. Bei einer Serververbindung sendet der PPC des EMVA-Clients das Fahrtziel, die kodierten Wunschmerkmale und ein Passbild-Icon.

6. Das Gerät des EMVA-Servers empfängt die Daten und zeigt sie im Display an, sofern die übertragenen Merkmale mit denen übereinstimmen, wie sie im Fahrer-Gerät abgelegt sind (internes Matching). Das Fahrer-Display bietet dabei die Möglichkeit, mehrere Anfragen untereinander darzustellen. Der Fahrer kann zwischen den Einträgen mit Hilfe von Navigationstasten (oder Sprachsteuerung?!) wechseln (scrollen).

   Ein gewählter Eintrag kann bearbeitet werden:
   a. grüne Taste: die Anfrage wird bestätigt. Der Client erhält auf dem Display seines PPC das Auto-Kennzeichen sowie ein Bild des Fahrers dargestellt. Liegen mehrere EVMA-Server-Bestätigungen vor, werden diese auf dem Display des Client-PPC untereinander angezeigt.
   b. rote Taste: der Eintrag wird auf dem Display gelöscht



7. Hierauf kann nun der EMVA-Client über eine grüne bzw. rote Taste die Rück-Bestätigung durchführen bzw. ablehnen. Es kann nur jeweils eine Rückbestätigung durchgeführt werden, da hierbei alle weiteren vom Server bestätigten Anfragen abgebrochen werden. Die davon betroffenen EMVA-Server erhalten davon Kenntnis. Die Einträge verschwinden daraufhin von deren Displays.

Erhält der EMVA-Server eine Rückbestätigung durch den Client, werden alle anderen Einträge vom Server-Display gelöscht und der bestätigte Eintrag vergrößert dargestellt. Der EMVA-Client erhält automatisch nochmals das Kennzeichen auf seinem Display angezeigt.

Der Fahrer hat die Möglichkeit, in Abständen von einigen Sekunden mehrere Anfragen zu bestätigen. Dabei bekommt der erste rückbestätigende Client den Zuschlag. Alle weiteren vom Fahrer bereits bestätigten EMVA-Clients erhalten automatisch eine Absage.
Es ist technisch sichergestellt, dass ein EMVA-Client nur jeweils eine Bestätigung rückbestätigen kann.

8. Der Mitfahrer steigt zu und überträgt mit einem Tastendruck auf den Startknopf auf seinem PPC eine Start-TAN für die Kontierung zum EMVA-Server. Auf dem Display des EMVA-Servers erscheint eine Zeit-Anzeige[1], welche die Startzeitpunkte für die Mitfahrer anzeigt.

Die laufende Zeit wird über einen Tastendruck des Client- oder Server-PPC angehalten. Dabei werden die aufgelaufenen Kontierungsdaten sowohl auf der Speicherkarte des EMVA-Servers wie auch auf der des Clients (als Bestätigung) abgelegt[2]. Sollte der Client beim Ausstieg die Quittierung vergessen, muss er sich sein Gerät beim EMVA-Betreiber für eine weitere Benutzung wieder freischalten lassen. Der Fahrer hingegen kann den Vorgang für den Mitfahrer abbrechen, aber die unvollständigen Daten nicht für eine Kontierung benutzen. In diesem Fall soll über den EMVA-Betreiber eine organisatiorische Lösung erreicht werden. Beide Parteien können daher aus einem Fehler der Gegenseite keinen Vorteil ziehen und haben daher ein Interesse am geregelten Geschäfts-Ablauf.

9. Der Fahrer überträgt zuhause die Kontierungsdaten mit Hilfe eines am PC angeschlossen Kartenlesegerätes von der Speicherkarte des EMVA-Gerätes via Internet zum EMVA-Betreiber. Dieser prüft die Gültigkeit der Daten und veranlasst einen entsprechenden Zahlungsvorgang (evtl. nur monatlich) nebst Provisionsabzug. Dabei wird sichergestellt, dass die selben Kontierungsdaten nicht mehrfach übertragen werden können[3]. Es wird sowohl für den Fahrer wie auch den Mitfahrer ein online abrufbarer Buchungsvorgang erzeugt.

[1] Alternativ können die aufgelaufenen Kosten dargestellt werden

[2] auf der Speicherkarte des EMVA-Servers verschlüsselt mit dem geheimen Schlüssel des EMVA-Clients (oder einem davon abgeleiteten Sitzungsschlüssels bzw. TAN) und umgekehrt. Damit sind nachträgliche Manipulationen ausgeschlossen.

[3] über Message Digest wie MD5

4. Technische Aspekte

- SmartCards bieten eine fälschungssicheren Speicherung von Daten, sofern das Kartenlesegerät vertrauenswürdig ist.
- Smartcards lassen sich mit einem Passbild bedrucken und kosten in Großserie (>100000 Stk) ca. 4€
- Private Speicherbereiche auf Smartcards können über eine PIN geschützt werden. Eine Anwendung wäre die Speicherung des privaten Schlüssels des Kartenbesitzers.
- Daten können auf Authentizität überprüft werden, wenn die Signatur-Schlüssel aus einer vertrauenswürdigen Quelle vorab bezogen werden können. Herr Meier kann damit Hr. Müller die Echtheit seines Ausweises „beweisen“, indem Hr. Müller Hr. Meiers öffentliche Daten (z.B. inkl. dessen darin abgelegtem Passbild) über sein Kartenlesegerät lädt und die kryptografische Quersumme davon bildet. Diese muss dann mit derjenigen übereinstimmen, die Hr. Müller in seiner vom Betreiber erhaltenen Datenbank gespeichert hat. Es ist zu prüfen, wie groß diese Datenbank bei einigen Millionen Einträgen wird!
- für die Client/Server-Kommunikation ist ein geeignetes Protokoll zu definieren und zu implementieren

5. Aufgaben/Risiken

- *Zuverlässigkeit:* WLAN-Kommunikation (Reichweite, Geschwindigkeit). Vorabtests mit zwei Netgear WG511 WLAN-Karten im ad-hoc Modus unter Linux ergaben eine ausreichende Reichweite von ca. 300m. Dabei war eine starke Abhängigkeit von der Richtung festzustellen, in welche die WLAN-Karten gehalten wurden. Dies ist für den konkreten Anwendungsfall aber eher als Vorteil zu betrachten!
- *Hardware:* Pocket PC's unterschiedlicher Hersteller unterscheiden sich z.T. stark. Es ist damit zu rechnen, dass Geräte-spezifische Anpassungen erstellt werden müssen.
- *Datensicherheit*. Insbesondere sind die Pocket PC's gegen Hacker-Attacken abzusichern. Welche kryptografischen Verfahren sind anzuwenden, um Mißbrauch mit Kontierungsdaten und personenbezogenen Daten auszuschließen? Sind Smartcards einsetzbar? Funktionsweise? Vorkehrungen für eine gesicherte Client-Server-Verbindung sind zu treffen (PK-Verfahren?!)
- *Performance*. (PK-Verfahren sind langsam)
- *Software-Architektur*: welche Entwicklungswerkzeuge/Sprachen Tools kommen zum Einsatz? (momentan wird C# mit dem .NET Compact Framework 1.0 favorisiert) .NET CF 2.0 steht allerdings schon in den Startlöchern (Visual Studio .NET 2005 Beta)!
- *Investitionsschutz*: läßt EMVA sich in essentiellen Teilen patentieren? Wie ist eine Kundenbindung möglich?
- *Produktname (z.B. der Domain*-Name trampware.com/de sind noch frei!)
- *Investitionen*: hier ist ein nicht unerheblicher finanzieller und organisatorischer Aufwand zu erwarten:
    - Marketing
    - Klärung rechtlicher Fragen (Patentrecht, Datenschutzrecht etc.)
    - Finanzierung (Anlaufkosten)
    - Partner
    - Hard-u. Software-Infrastruktur (Web, Datenbank, Support)