Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Studienarbeit

ePayment in Ferienclubs: Entwurf eines ePaymentsystems unter Nutzung von PDA's

vorgelegt von
Jan Szensny
am 28. April 2005

Studiengang Softwaretechnik

Betreuender Prüfer: Prof. Dr. Kai von Luck

Fachbereich Elektrotechnik und Informatik
Department of Electrical Engineering and Computer Science

ePayment in Ferienclubs: Entwurf eines ePaymentsystems unter Nutzung von PDA's

Stichworte ePayment, Payment, Zahlmethoden, Ferienclubs, Zahlung, Kredit, PDA, eWallet, eCash

Zusammenfassung

Immer weiter drängen sich Begriffe wie ePayment und Wireless in die Köpfe der Leute, Also warum nicht mal diese beiden Begriffe für einen Ferienclub zusammenfassen?
In dieser Arbeit soll gezeigt werden wie ein mögliches ePayment-System für einen Ferienclub aussehen könnte. Hierbei werden Einzellösungen wie eWallet (eGeldbörse) und ePayment (eGuthabenkonto) betrachtet und zu einem anderen System (eCreditcard) zusammen gesetzt. Gleichzeitig werden einige weitere Punkte die es in einem Ferienclub zu bedenken gilt angesprochen und mit ersten Lösungsmöglichkeiten versehen.
Zum Abschluss stellen wir dar wie das hier entwickelte System in der Realität aussehen könnte.

ePayment in Ferienclubs: Entwurf eines ePaymentsystems unter Nutzung von PDA's

Keywords ePayment, payment, Club Holiday, Credit, PDA, eWallet, eCash

Abstract

In this document we are going to demonstrate a possible ePayment system for a holidays club. First we show single solutions as eWallet and ePayment which will be combined to another system, the eCreditcard. There are also some further points in a holidays club to consider, for which we will work out first solutions. Finaly we're going to explain how this system could look like when it is realized.

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Einleitung

Als kurze Einleitung in das Thema dieser Studienarbeit wird zunächst eine kurze Zeitreise unternommen, in der beschrieben wird, auf welche Weise bisher in Ferienclubs bezahlt wurde. Hierbei gilt zu beachten, das es sich nur um bargeldlose Zahlungen innerhalb des Clubs bzw. Clubnetzwerkes handeln soll.

1.1. Vergangenheit

In der Anfangszeit der bargeldlosen Zahlung in Ferienclubs wurden in den einzelnen Clubs jeweils Unternehmensspezifische Tauschmittel wie z. B. farbcodierte Perlen, Bändchen oder Coupons verwendet.

Dieser einfache Austausch der verwendeten Tauschmittel (Perlen statt echtem Geld) stellte effektiv gesehen eine Clubinterne, eigene Währung dar, mit all ihren Vor- wie Nachteilen. So waren die Clubgäste dazu gezwungen sich an eine weitere Währung in Ihrem Urlaubsort zu gewöhnen. Andererseits bestand für die Clubgäste bei dieser Methode die Möglichkeit Transaktionen mit anderen Personen durchzuführen ohne daß der Club für diese Transaktionen einbezogen werden musste. Gleichzeitig bestand aber das Risiko für die Gäste, das diese bestohlen werden konnten und ggf. erst beim nächsten Zahlungsvorgang den Verlust bemerkten, wenn überhaupt. In einem solchen Fall gäbe es keine Möglichkeit für den Club oder den Gast, den Verbleib des „Geldes“ nachzuvollziehen.

1.2. Gegenwart

Da inzwischen die Technik weiter fortgeschritten ist und entsprechende Systeme immer stärkere Verbreitung finden, wurde bereits vor einiger Zeit in vielen Clubs eine neue, modernere Technik zum Einsatz gebracht. So bieten heutzutage die meisten Ferienclubs Ihren Gästen ein System, mit dem sie sich auf eine einfache Art und Weise jederzeit dem Club gegenüber identifizieren können und gleichzeitig innerhalb des Clubs Zahlungen leisten können. Hierzu werden Systeme vergleichbar mit „Geldkarten“ eingesetzt. Auf dem Chip dieser „Clubausweise“ werden alle gastspezifischen Daten gespeichert, wodurch z. B. in einem Fall das

nicht genügend Guthaben auf der Karte vorhanden ist, der zuzahlende Betrag auf die Zimmerrechnung des Gastes geschrieben werden könnte, ohne daß der Gast mehr tun muss als eine entsprechende Quittung zu unterzeichnen.
Die Probleme dieses Systems bestehen zum einen in der Komplikation, daß der Gast nicht ohne entsprechende Terminals den aktuellen Stand seines Guthabens einsehen kann, zum anderen in der immer noch bestehenden Problematik das Guthaben gestohlen werden könnte.
Als Vorteil könnte bei diesem System jedoch gewertet werden, dass eine entwendete Karte sofort nach bemerken gesperrt werden könnte und eine weitere unrechtmäßige Verwendung des Kartenguthabens dadurch vermieden werden könnte.
Jedoch sollten bei der Verwendung eines solchen Systems alle Transaktionen geloggt werden, wodurch einerseits das Guthaben des Gastes wiederherstellbar wäre, andererseits die Nutzung einer entwendeten Karte zurückverfolgt werden könnte.

1.3. Zukunft

Mit einer möglichen zukünftigen Methode soll sich diese Studienarbeit beschäftigen. Hierzu soll als Grundlage angenommen werden, daß jedem Gast des Ferienclubs während seines Aufenthaltes ein PDA zur Verfügung gestellt wird, mit dessen Hilfe er bereits angebotene Dienste wie z. B. Tages-/Wochenpläne, Menükarten, Lagepläne, etc. nutzen kann. Um in diesem Zusammenhang eine Möglichkeit zu bieten, über die der Gast bargeldlos Rechnungen innerhalb des Clubs begleichen kann, soll das angenommene Grundsystem um ein autonomes ePayment-System erweitert werden, wobei die Vorzüge aller bisherigen Systeme zu einem neuen System vereinigt werden sollen.

So soll dem Clubgast die Möglichkeit geboten werden auf eine möglichst einfache aber sichere Weise innerhalb des Clubs Zahlungen zu tätigen, wie z. B. Getränke an der Bar bezahlen oder andere kostenpflichtige Angebote nutzen.

2. Analyse

2.1. Die Grundidee

Wie bereits in der Einleitung beschrieben, soll diese Studienarbeit ein mögliches System für den bargeldlosen Zahlungsverkehr in Ferienclubs beschreiben. Hierbei sollen nach Möglichkeit die Vorteile der bisherigen Zahlungsmethoden zu einer neuen, bequemen und sicheren Methode zusammengefasst werden.

2.2. Systemaufbau-Möglichkeiten in der Theorie

Für die Planung dieses Systems werden zwei mögliche Strukturen vorgestellt.
Als erstes soll eine Möglichkeit betrachtet werden, bei der das Guthaben des Gastes lokal auf seinem PDA verwaltet wird.
Im Anschluss daran wird die zentrale Verwaltung aller Gast-Guthaben auf einem Club-internen Server betrachtet.
Beide Verfahren werden im Anschluss an die Beschreibungen nochmals graphisch Gegenübergestellt (siehe 2.2, S.11).

Nach der getrennten Betrachtung der beiden Verfahren werden erste Vor- und Nachteile im direkten Vergleich aufgezeigt um abschließend eine mögliche Kombination beider Verfahren vorzustellen, in der bereits erste Erweiterungen berücksichtigt werden.

eWallet - Guthaben auf dem PDA

Diese erste Möglichkeit, die „elektronische Geldbörse“ (eWallet), würde nach dem Beispiel der in der Einleitung beschriebenen Geldkarte realisiert werden. Hierbei kann der Clubgast seinen PDA bei Mitarbeitern des Clubs, z. B. an der Rezeption, mit einem Guthaben aufladen. Ein ggf. einzurichtender Code zur Freigabe einzelner Transaktionen würde lokal auf dem PDA gespeichert werden und bei Bedarf zum Abgleich und zur Freigabe von Transaktionen verwendet werden. Bei allen Transaktionen würde der PDA vom Clubnetz bzw. einem Server des Netzes mitgeteilt bekommen, was dieser zu tun hat, z. B. bei einer Aufladung des Guthabens gäbe es die Nachricht den entsprechenden Betrag als Einzahlung zu verbuchen, dies bedarf keines weiteren eingreifens durch den Gast. Aufgrund der lokalen Speicherung aller „Geldbörsen“ Daten direkt auf dem PDA wäre der Gast jederzeit in der Lage seinen aktuellen Guthabenstand abzufragen oder ggf. die durchgeführten Transaktionen zu betrachten um sich über den Verbleib seines Guthabens zu informieren.

Bei allen Transaktionen hingegen, welche ein abgehen von Guthaben vom PDA bewirken, muß sich der PDA beim Gast vergewissern ob die jeweilige Transaktion, die getätigt werden soll, korrekt ist. Im Fall, daß die Transaktion vom Gast gewollt ist, autorisiert dieser die Transaktion durch die Eingabe des persönlichen Identifikationscodes, welcher lokal auf dem PDA gespeichert ist und nicht für externe Dienste zugänglich ist. Anschließend wird das Guthaben des Gastes um den entsprechenden Betrag verringert, ein entsprechender Eintrag in die Transaktionsliste aufgenommen und eine Durchführungsbestätigung an den Auftraggeber gesendet.

Sollte die Transaktion jedoch nicht korrekt sein, so wird diese durch den Gast abgebrochen und der PDA informiert den Auftraggeber über die Ablehnung der Transaktion.

Generell sollten alle Transaktionsanfragen protokolliert werden, um evtl. Missbrauch des Systems verfolgen zu können.

Vergleichbar mit: Geldkarten

eCash - Guthaben auf einem Server

Als zweite Möglichkeit bietet sich ein zentralverwaltetes Guthabenkonto ähnlich einem „Bankkonto“ an. Dieses würde verwendet werden wie ein herkömmliches Bankkonto. Sämtliche Transaktionen würden über einen clubinternen Server erfolgen, wodurch zur Nutzung des eigenen Guthabens bzw. zur Abfrage des Guthabenstandes oder der Transaktionsliste eine Verbindung zum Clubnetzwerk gegeben sein muß. Sobald sich der Gast außerhalb der Reichweite des Clubnetzwerkes befindet, ist es für ihn weder möglich Transaktionen durchzuführen, z. B. mit anderen Clubgästen, noch kann er sein Guthaben bzw. die erfolgten Transaktionen betrachten. Zwar gibt es die Möglichkeit diese Daten ebenfalls auf dem PDA vorzuhalten, jedoch muß in einem solchen Fall eine ständige Synchronisation mit den Daten auf dem Server erfolgen, wodurch weitere Probleme auftreten könnten, wie z. B. durch eine „verspätete“ Synchronisation, wobei eine getätigte Transaktion erst zu einem späteren Zeitpunkt mit dem PDA abgeglichen werden könnte und der Gast durch dieses verspätete Auftauchen dieser ihm evtl. entfallenen Transaktion irritiert wird.

Im Gegensatz zur *eWallet* kann die Speicherung des Berechtigungscodes bei diesem System alternativ ebenfalls auf einem weiteren clubinternen System erfolgen, wodurch eine detailliertere Rechteprüfung erfolgen kann. Durch diese Auslagerung der Rechteprüfung würde ein Problem aufgrund der Kompromittierung eines PDA vermieden, gleichzeitig jedoch eine weitere mögliche Angriffsstelle geschaffen werden.

So müssten die vom PDA an den Clubserver übermittelten Daten extra verschlüsselt werden um die Entwendung der Zugriffscodes zu vermeiden. Gleichzeitig darf dieses Verschüsselungsverfahren nicht zu rechenintensiv werden, da bei beinahe jeder Transaktion zwischen dem PDA und dem Server die übertragenen Daten verschlüsselt werden müssten und diese Übertragungen keine unnötige Beeinträchtigung des PDA, des Servers oder gar des gesamten Clubnetzwerkes nach sich ziehen dürfen.

Für den Clubgast stellt sich dieses System in der Nutzung nicht viel anders dar als die *eWallet*-Lösung, jedoch gibt es für den Gast keine Möglichkeit zur Durchführung von Transaktionen, wenn das Clubnetzwerk nicht zur Verfügung steht, egal ob sich der Gast außerhalb des Netzwerkes befindet, oder ob Netzwerkprobleme die Verbindung verhindern.

Da jedes dieser beiden Verfahren seine Vor- sowie Nachteile bietet, wurde über eine Vereinigung beider Systeme nachgedacht, welche im nun folgenden Abschnitt beschrieben werden soll.

Vergleichbar mit:

- Internet Bezahlsystemen z.B.: Paypal, Moneybookers
- Guthabensystemen: ExportForce2 von Klamm.de und ähnliche

eWallet und eCash - Ein Vergleich

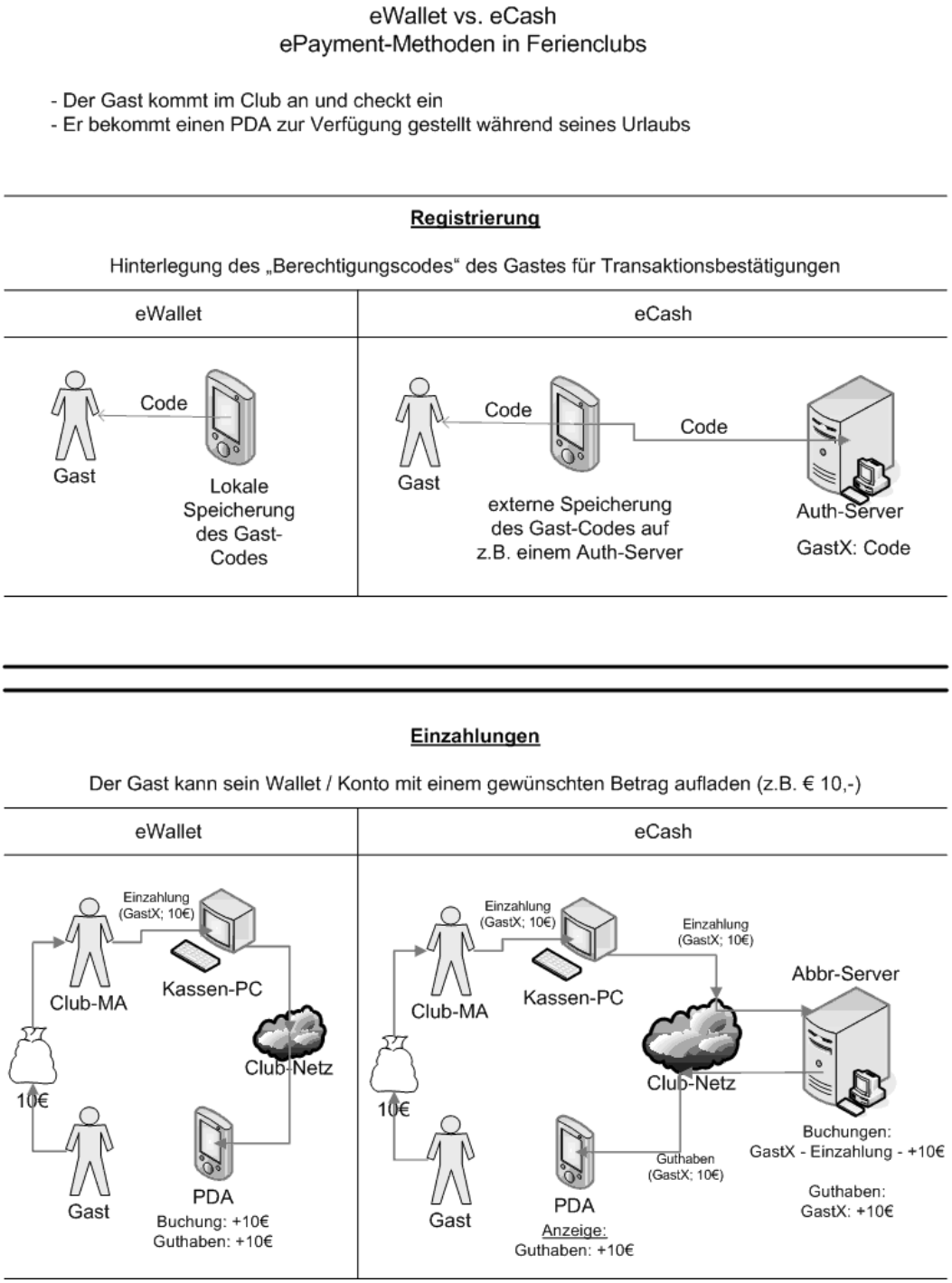

Abbildung 2.1.: Ein Vergleich von eWallet und eCash - Registrierung und Einzahlungen

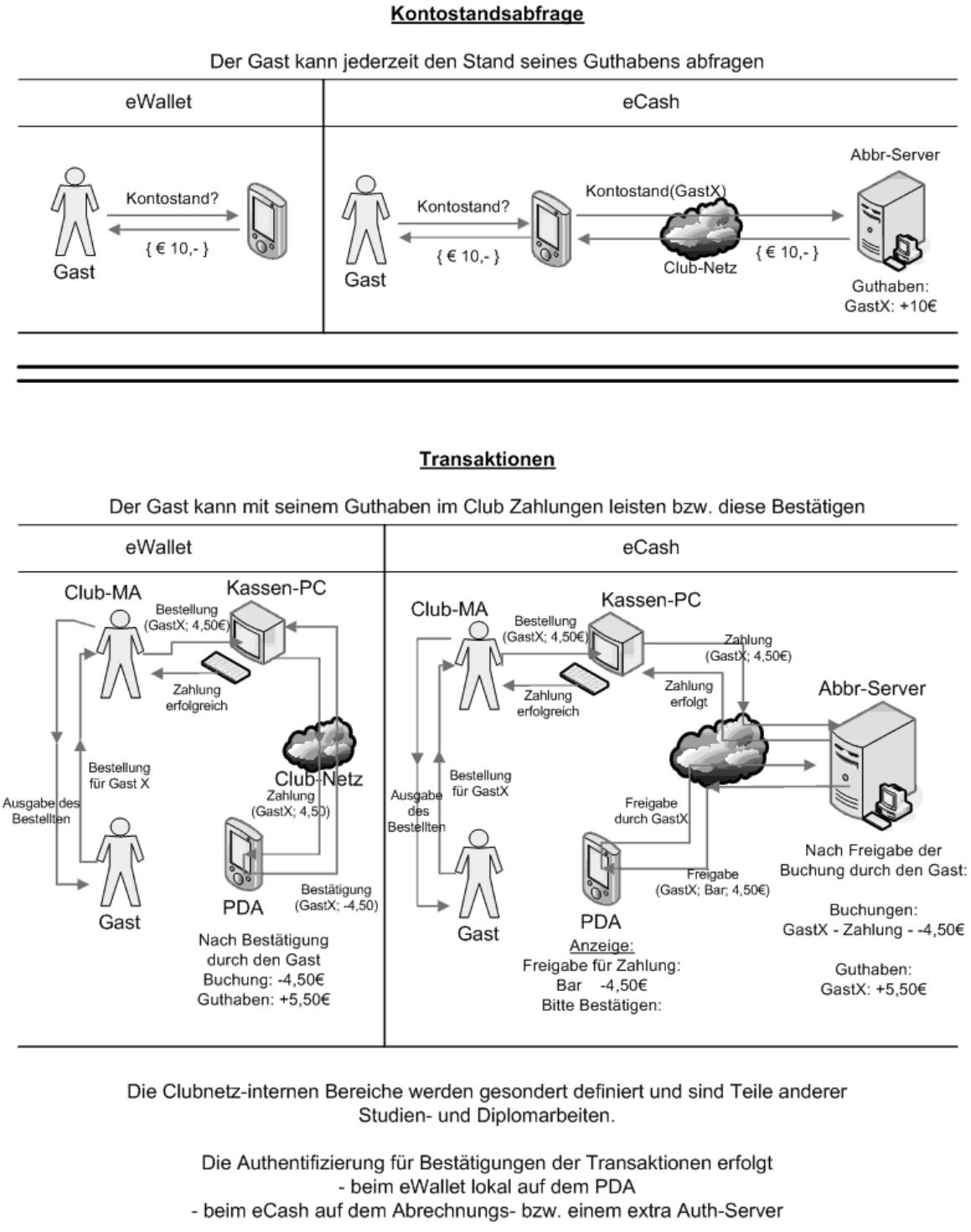

Abbildung 2.2.: Ein Vergleich von eWallet und eCash - Kontoabfragen und Transaktionen

2.3. eCredit - Ein angepasstes System

Die Überlegung hinter diesem Lösungsvorschlag bestand darin, daß dem Gast die Möglichkeit geboten werden sollte, auch außerhalb des Clubnetzwerkes mit dem PDA Zahlungen leisten zu können. Gleichzeitig sollte gewährleistet bleiben, daß der Gast innerhalb des Clubnetzwerkes auch Zahlungen tätigen kann, wenn seine „elektronische Geldbörse“ nicht genügend gefüllt ist. Hierbei sollte sich das Verfahren für den Gast nicht ändern, d.h. auch weiterhin soll der Gast durch einfache Eingabe seines Codes eine Transaktion tätigen können, wobei jedoch ggf. die Möglichkeit besteht, einen entsprechenden Hinweis anzugeben, daß das „Kreditkonto“ des Gastes belastet wird.

Zwei bisher in die Überlegungen einbezogene Verfahren sind die folgenden:

1. die eWallet wird genutzt bis das Guthaben aufgebraucht ist, anschließend wird das eCash-Verfahren verwendet
2. eine Erweiterung der ersten Überlegung, bei der nach Verbrauchen des Guthabens bis zu einem vorgegebenen Limit weiterhin die eWallet genutzt wird, erst nach erreichen dieses Limits wird auf das eCash-Verfahren umgestellt.

Vergleichbar mit: Kreditkarten

2.4. Erweiterungen

Spätestens in dem Moment, wenn die erste Familie mit ihren Kindern eincheckt und eben jeder Gast einen eigenen PDA zur Verfügung gestellt bekommt, werden die ersten Probleme, die bisher noch nicht betrachtet wurden, auftreten. Der Einfachheit halber wollen wir annehmen das Kindern und Jugendlichen ab 12 Jahren ein eigener PDA zur Verfügung gestellt werden kann, sofern dies von den Eltern gewünscht wird.

Trotzdem ist es in der Regel von den Eltern nicht gewünscht, daß die Kinder das zur Verfügung gestellte Guthaben unkontrolliert ausgeben. So sollte Eltern die Möglichkeit gegeben werden über das Guthaben ihrer Kinder zu Verfügen, um z.B. das gesamte Guthaben des Kindes zu sperren oder Regeln bzw. Limits einstellen zu können.

Andererseits gibt es auch Gäste die sich selbst z. B. Tageslimits setzen wollen, um nicht ihr gesamtes Guthaben an einem Tag auszugeben.

Diese und weitere Themen sollen in den nun folgenden Abschnitten mit entsprechenden Lösungsansätze aufgezeigt werden.

Rechte - Vormund-/Vertretungsberechtigung

Das erste und für Eltern wohl mit das wichtigste Thema dürfte sein: „Wie kann ich die Verwendung des Guthabens meines Kindes überwachen?“

Generell sollte es möglich sein, mehreren Personen die Berechtigung zu erteilen, über das Guthaben eines Gastes zu verfügen. So sollte es eingerichtet werden, daß der Partner eines Gastes die volle Verfügungsberechtigung über das Guthaben des Gastes hat. Andererseits sollten Einschränkungen möglich sein, anhand derer die Eltern eines jugendlichen Gastes z. B. keine Verfügungsgewalt über das Guthaben des Sprösslings haben, jedoch die Verwendungszwecke oder Limits regeln können. Gleichzeitig könnten diese Rechte dem Sprössling, dem Inhaber des Guthabens, entzogen werden.

Privattransfers - Austausch von Guthaben zwischen Gästen

Häufig kommt es vor, daß nicht jeder Gast aus einer Gruppe seinen eigenen PDA bei sich hat und eine andere Person alle Zahlungen übernimmt. Um nun nicht jedesmal mit dieser Person zur Rezeption gehen zu müssen und einzelne Beträge auf sein Guthabenkonto aufzuladen, sollte die bequeme alternative von Guthabentransfers zwischen Gästen ermöglicht werden. Hierbei sollte es genügen, wenn der „überweisende“ Gast nur den empfangenen Gast sowie den zu übertragenden Betrag eingibt und diese Transaktion mit seinem Freigabecode bestätigt.

Für den empfangenden Gast sieht eine solche Transaktion aus wie eine herkömmliche Einzahlung. Der überweisende Gast kann in seiner Transaktionsliste jederzeit sehen, wann er welchen Betrag an wen übertragen hat.

Token - Zweckbindung von Guthaben

Angenommen eine Familie mit einem 14jährigen Sohn verbringt Ihren Urlaub in diesem Ferienclub. Die Eltern möchten Ihrem Sohn ein „Taschengeld“ auf sein Konto aufladen, jedoch soll sichergestellt sein, daß der Sohn dieses Geld nicht für alkoholische Getränke[1] ausgibt.

Für diesen Fall ist ein Tokensystem empfehlenswert, welches einzelne Verwendungszwecke für das Guthaben ermöglicht. So könnten verschiedene Token eingerichtet werden, welche besagen, daß ein bestimmter Teil des Guthabens explizit für alkoholische Getränke, Internet surfen, etc. freigeschaltet wird.

[1] In der Regel sollte der Ausschank von alkoholischen Getränken an minderjährige bereits von den Barmitarbeitern abgelehnt werden.

Gleichzeitig sollte es die Möglichkeit geben einzelnen Token eine Gültigkeitsdauer zuzuweisen, wodurch diese Token nur bis zum Ablauf dieses Zeitpunktes gültig sind und anschließend gesperrt werden. Als Beispiel könnte sich ein Gast ein tägliches Limit setzen, bis zu welchem er alkoholische Getränke erwerben könnte.

Nach Verbrauch diesen Guthabens gäbe es mehrere Möglichkeiten,

1. dem Gast wird bei überschreiten des Limits eine entsprechende Meldung ausgegeben
2. jede Zahlung, welche das Guthaben übersteigt, wird verweigert

Hierbei dürfte die erste Möglichkeit für einen durchschnittlichen Gast die empfohlene sein, da er sich ansonsten bevormundet vorkommen könnte, selbst wenn das Limit und die Einschränkung von ihm selbst gesetzt wurden. Die zweite Möglichkeit wäre hingegen für Kinder bzw. Jugendliche (und andere Personen) empfehlenswert, wenn der Erwerb von nicht freigegebenen Dingen generell verweigert werden soll.

Ebenfalls interessant wäre die Möglichkeit zeitlich begrenzte Limits zu setzen, wie z. B. ein tägliches Limit, wobei nur Guthaben verwendet werden kann, bis dieses Limit überschritten wurde. Weitere Transaktionen werden abgelehnt.

Im Rahmen dieses Tokensystems würde sich gleichzeitig die Möglichkeit bieten, daß der Club „Spezial-Token“ ausgibt, welche den Gast dazu bemächtigen spezielle, begrenzte Angebote zu nutzen, wie z. B. wöchentlicher Besuch eines Spezialitäten Restaurants, Nutzung der Tennisanlagen bzw. des Wassersportangebotes, etc..
Im Zusammenhang mit diesen „Spezial-Token“ wäre die Gültigkeitsdauer eine wichtige Eigenschaft, da diese Art von Token in der Regel nur für einen bestimmten Zeitraum gültig sein sollte und der Gast diese normalerweise nicht sammeln dürfte. Gleichzeitig sollte es für jeden Tokentyp einzeln entscheidbar sein, ob diese zwischen Gästen transferiert werden dürfen oder nicht.

Für die regelmäßigen und automatischen Erneuerungen der z. B. Limits oder Spezial-Token, sollten einzelne Automatismen eingerichtet werden, welche dafür sorgen, daß die Limits täglich neu gesetzt werden bzw. aktualisiert werden. Ebenfalls sollten die „Spezial-Token“ bei Bedarf automatisch aktualisiert bzw. ausgetauscht werden.

Für diese „autoUpdates“ müsste jeweils geprüft werden, durch wen das jeweilige Update erfolgen sollte. Wird es durch den Clubserver ausgeführt, z. B. die Aktualisierung der „Spezial-Token“, oder kann die Updatefunktion auf den PDA des Gastes ausgelagert werden, z. B. bei den Limits.

Vergleichbar mit: Digital Rights Management (DRM)

3. Anforderungen

Nachdem nun die erste Analyse abgeschlossen ist, gilt es zu überlegen welche Komponenten zur Realisierung dieses Projektes benötigt werden.
Hierzu wird in diesem Kapitel jeweils ein kurzer Blick in die einzelnen Bereiche geworfen und die jeweiligen Anforderungen bestimmt.

Der Bereich Hardware wird schnell durchschritten sein, da für die Integration der Serversoftware, wie z.B. den Abrechnungsserver oder ggf. auch einen Authentifikations-Server, Kapazitäten auf bereits vorhandenen Servern verwendet werden können.
Auf die zusätzlich benötigten PDA's braucht in diesem Fall nicht vertieft eingegangen werden, da in der Regel die heute erhältlichen Geräte alle Mindestanforderungen bereits in der Grundausstattung erfüllen oder gegebenenfalls leicht nachrüstbar sind.

Den Bereich Software werden wir ein wenig detaillierter Betrachten, da es hier besonders zu bedenken gilt, wie die einzelnen Softwarekomponenten miteinander kommunizieren sollen. So muß in diesem Bereich überlegt werden, ob die Softwarekomponente welche den Bestätigungsdialog auf dem Gast-PDA bereitstellt mit der Unterstützung durch einen ORB-Dienst implementiert werden soll oder ob hierfür eine eigene „Client-Verwaltung" benutzt werden soll, mit deren Hilfe ein Server mit dem „richtigen" PDA eine Verbindung herstellen kann. Zusätzlich werden wir in diesem Abschnitt noch versuchen zu klären, welche Softwarekomponenten für die Realisierung dieses Projektes benötigt werden.

Abschließend werden wir uns einem Bereich zuwenden, bei dem es schwer fällt einen Trennstrich zwischen den beiden Teilbereichen zu ziehen, Netzwerk und Sicherheit.
Da dieser Bereich bereits in mehreren anderen Arbeiten betrachtet wurde, werden wir an dieser Stelle nicht allzu tief einsteigen, und die einzelnen Punkte nur kurz streifen.
Zu Beginn werden wir kurz verschiedene Netzwerkmedien betrachten und eventuelle Sicherheitsbedenken ansprechen. Nachfolgend werden wir kurz verschiedene Authentifizierungsmöglichkeiten aufzeigen um abschließend kurz auf ein zur Zeit durchgeführtes Test-Projekt zu verweisen, welches für dieses Thema als Erweiterung implementierbar sein könnte.

Abgeschlossen wird dieses Kapitel mit einem „architektonischen Big-Picture" in dem die bisher festgelegten Eigenschaften in Form einer möglichen Netzwerk-Architektur grob skizziert dargestellt werden soll.

3.1. Hardware

Wie in der Einleitung dieses Kapitels bereits erwähnt wird dieser Abschnitt schnell durchschritten sein.

Als Hardware wird für dieses Projekt mindestens ein Server benötigt, welcher jedoch auch bereits andere Dienste zur Verfügung stellen kann. Auf diesem Server soll der Abrechnungsservice bereitgestellt werden, der sämtliche Kontoverwaltung übernimmt.

Zusätzlich werden für die Clubgäste noch PDA's benötigt, mit deren Hilfe die Kontofunktionen verwendet werden können. Als Anschauungs- und Test-PDA stand für dieses Projekt ein *HP iPAQ Pocket PC H5550* zur Verfügung.

Nicht zu vergessen seien an dieser Stelle die benötigten Terminals, die von den Mitarbeitern des Clubs als Kassen eingesetzt werden können. Diese Terminals könnten im Grunde aus jeder Netzwerkfähigen Hardware bestehen, auf der eigene Software ausgeführt werden kann. So könnten sogar die Mitarbeiter des Clubs PDA's zur Verfügung gestellt bekommen, auf denen dann jedoch eine angepasste Software laufen müsste.

Weiterhin ist natürlich noch ein funktionsfähiges Netzwerk von Nöten, welches eine sichere Kommunikation zwischen den Geräten ermöglicht.

Benötigte Hardware für die Realisierung:

- Server zur Bereitstellung des Abrechnungs- sowie ggf. Authentifizierungs-Services
- PDA's für die Gäste, mit deren Hilfe Transaktionen getätigt werden können
- Terminals, die als Kasse bzw. Abrechnungsstationen dienen und Transaktionen initiieren.

3.2. Software

Bei diesem Projekt gilt es mindestens vier Softwarekomponenten zu entwickeln.

- Abrechnungsservice (Server)
- PDA-Clients (PDA)
- „Push-to-Pay“-Service auf dem PDA
- Kassensoftware (Terminal)

Weitere Softwarekomponenten sind möglich und könnten sich während der Realisierung als erforderlich erweisen.

Server-Software

Abrechnungsservice

Als Hauptbestandteil der Serverseite sei hier der Abrechnungsserver selbst genannt. Dieser Service stellt die einzelnen Konten der Gäste sowie die Token selbst zur Verfügung und wird bei allen beschriebenen Implementierungen in unterschiedlichem Umfang Verwendung finden.
So stellt dieser Service bei der reinen eWallet-Lösung ein Token/Guthaben-Depot des Clubs dar, in dem nicht verwendete Token „gelagert“ werden bzw. bei Bedarf neue Token generiert werden können. In diesem Szenario bietet der Abrechnungsservice dem Club jederzeit den Überblick darüber, wie viele Token bzw. wie viel Guthaben derzeit im Umlauf sind.
Weiterhin sollte dieser Abrechnungsservice Schnittstellen bieten, mit deren Hilfe z.B. Client-Software nachgerüstet werden könnte, die weitere Funktionen, besonders für den kaufmännischen Bereich, bieten würde.

sonstige Server-Software

Im nachfolgenden Abschnitt Netzwerk und Sicherheit (3.3) werden wir kurz auf einen Authentifikations-Service eingehen, welcher zusätzlich im Netzwerk bereitgestellt werden könnte und als „sicherer Dienst„ die Authentifizierung der Transaktionsfreigaben übernehmen könnte.

Client-Software

Clients - Kontostände, Umsätze und andere Transaktionen

Auf dem PDA des Gastes wird ein Client benötigt, welcher die Verbindung zum Abrechnungsservice (oder anderen Services) herstellen kann um Kontoinformationen, wie z.B. Kontostände, Umsätze oder andere Informationen, vom Server abzurufen und auf dem PDA darzustellen.

Vergleichbar mit: Online-Banking

„Push-to-Pay“-Dienst auf dem PDA

Die „Push-to-Pay“-Funktion soll es ermöglichen, daß z.B. ein Abrechnungsservice die Bestätigung einer Transaktion vom PDA des entsprechenden Gastes anfordert. Hierbei muß eine Zuordnung zwischen Gast und PDA existieren, wodurch die Clubservices jederzeit wissen, welcher Gast über welchen PDA erreichbar ist.
Um dieses Wissen zu gewährleisten sollte bei der Ankunft eines Gastes eine feste Zuordnung zwischen Gast und PDA erfolgen. Diese Zuordnung könnte in einer einfachen Datenbank hinterlegt werden, auf die alle Services lesenden Zugriff erhalten könnten.
Zusätzlich bleibt an dieser Stelle zu überlegen, in welcher Art die Kommunikation zwischen einem Service und einem PDA erfolgt. Genügt ein einfaches Anfrage-Antwort-Protokoll, bei dem der Service eine TCP-Verbindung zum PDA aufbaut und die Bestätigung anfordert und nach Erhalt der Antwort die Verbindung wieder beendet, oder soll eine Objekt basierte Lösung in Form eines ORB's[1] verwendet werden.

Unabhängig von der endgültigen Realisierung würde dieser Dienst die Aufgabe haben, auf Bestätigungsanforderungen der Services zu warten und sofern eine eintrifft, die Freigabe von seinem Nutzer einzuholen, dessen Ergebnis er an den anfordernden Service zurückmeldet.

Vergleichbar mit: Verfahren zur Bestätigung von Handy-Nr.

[1] ORB - Object Request Broker - z.B. CORBA

Terminal-Software

Kassen-Software

Nicht zu vergessen sei an dieser Stelle die Kassen-Software, mit deren Hilfe die Club-Mitarbeiter Transaktionen zwischen Club und Gast veranlassen können.
Hierbei sei anzumerken, daß diese Terminals nur wenige Funktionen bieten müssen. So werden hier nur die einzelnen Teile der Bestellung gesammelt um sie abarbeiten und abrechnen zu können.
Für die Veranlassung der Transaktion wären demnach nur zwei Angaben erforderlich:

- Liste der Artikel mit Preisen bzw. Endpreis
- Gast-ID

Diese Informationen würden an den Abrechnungsservice übermittelt werden, woraufhin dieser die Transaktion durchführen und das Endergebnis an das entsprechende Terminal zurückmelden würde.

Zusätzlich wäre noch zu überlegen, ob diese Kassen-Software derart erweitert wird, daß mit Ihrer Hilfe Abschlüsse erstellt werden können.

3.3. Netzwerk und Sicherheit

In diesem Abschnitt wollen wir auf die drei Punkte *Netzwerk, Sicherheit und Authentifizierung* eingehen. Da die Bereiche Netzwerk und Sicherheit, wie erwähnt, bereits in anderen Dokumenten[2] detailliert ausgearbeitet wurden, werden wir diese Teilbereiche hier nur kurz ansprechen.
Anders sieht es jedoch beim Bereich Authentifizierung aus, da dieser bei einer späteren Realisierung eine bedeutende Rolle spielen könnte.

[2] Verweise auf diese Dokumente sind im Anhang hinterlegt.A.1

Das Netzwerk

Das Medium

Heutige PDA's bieten in der Regel bereits von sich aus mehrere Kommunikationsmedien an oder stellen zumindest die Möglichkeit bereit entsprechende Adapter nach zurüsten.
Ein heute handelsüblicher PDA bietet neben der Möglichkeit sich über die zugehörige Dockingstation an einen PC anschließen zu lassen zusätzlich die Möglichkeiten der drahtlosen Vernetzung. Hierbei stellen die Geräte zwei Medien zur Auswahl an:

- Bluetooth und
- Wireless LAN

Effektiv spielt das verwendete Medium bei der Realisierung dieses Projektes eine untergeordnete Rolle, da beide Medien i.d.R. nicht direkt von der zu entwickelnden Software angesprochen werden, sondern vollständig unter der Kontrolle des Betriebssystems bleiben. Jedoch sollte bei der Realisierung des Projektes ein Medium festgelegt werden um spätere Komplikationen durch die Verwendung des „falschen" Mediums zu vermeiden.

Die Sicherheit des Mediums

Wie bei jedem Netzwerk darf auch bei der Realisierung dieses Projektes die Absicherung des Netzwerkes nicht zu kurz kommen. Jedoch sollen in diesem Zusammenhang hier nur kurz generelle Problematiken beim Betrieb dieses Netzwerkes angesprochen und aufgezeigt werden. Die detailliertere Behandlung von Lösungen für diese Probleme wird z.B. in „Sicheres Wlan im Ferienclub" von R.Bartnik (siehe A.1) dargelegt.

Da in diesem Netzwerk teilweise sensible Daten übertragen werden, die nicht unbedingt für die Augen Ditter zugänglich sein sollten, sollten alle hier verwendeten Medien bereits ein Mindestmaß an eigener Absicherung des Datenverkehrs mit sich bringen.
So sollte gewährleistet sein, daß sich kein Fremdes, unberechtigtes Gerät in das Clubnetzwerk einbinden kann um Funktionen oder Services des Clubs zu nutzen. Ebenfalls muß gewährleistet sein, daß ein „lauschendes" Gerät keine interpretierbaren Daten mitschneiden kann, d.h. jede Kommunikation sollte zumindest durch eine Funktion des Mediums oder extra bereitgestellte Software (z.B. VPN) gesichert werden.

Die Sicherheit

Dieser Themenbereich dürfte ebenfalls einer der wichtigsten bei der Umsetzung sein, wurde jedoch ebenfalls bereits in der Arbeit von A.Lüpke - „Entwurf einer Sicherheitsarchitektur für den Einsatz mobiler Endgeräte“ (siehe A.1) erläutert.

Daher sollen an dieser Stelle nur kurz einige Sicherheitsrelevante Punkte angedeutet werden, auf die bei der Realisierung besonders geachtet werden sollte.

1. Stammt die Anforderung vom richtigen Server?
2. Hat der Server die richtigen Daten übermittelt?
3. Sind die Daten beim Server bzw. PDA angekommen?
4. Ist der angeforderte PDA zur Zeit aktiv (ist er an) ?

In der Regel kann davon ausgegangen werden, daß ein Gast der einen PDA bedient sich in das Gerät eingeloggt hat und somit feststeht, daß dieser Gast die nötigen Rechte bei diesem Gerät besitzt. Eine weitergehende Authentifizierung bei der Freigabe von Transaktionen ist in diesem Fall also nicht von nöten.
Anders sieht dieser Punkt jedoch beim Einsatz einer Vormundschafts-/Vertretungsfunktion 2.4 aus, hier müssen höhere Berechtigungen separat bei jeder Transaktion freigeschaltet werden. Daher würden an dieser Stelle nur die Funktionen bzw. Rechte beim eingeloggten Nutzer automatisch aktiv sein, die alle Nutzern des Gerätes besitzen. Die jeweils höheren Rechte einzelner Nutzer müssten bei jeder einzelnen Transaktionen immer wieder erneut freigeschaltet werden.

Die Authentifizierung

Wenn man damit anfängt sich Gedanken über das Thema Authentifizierung zu machen, werden einem als erstes unterschiedlichste Verfahren einfallen, mit deren Unterstützung die Berechtigung einer Person geprüft werden könnte.
Diese unterschiedlichsten Verfahren nutzen jeweils Schlüssel einer der drei folgenden Gruppen:

- know - Schlüssel die man kennt (PIN, Passwort)
- have - Schlüssel die man besitzt (Karten, (Tür-)Schlüssel)
- be - Schlüssel die aus der Person selbst bestehen (biometrischer Schlüssel - Iris, Fingerabdruck, Stimme)

Während der Überlegungen zu dieser Arbeit sind bisher vier Verfahren zur Abgabe einer nachvollziehbaren Willenserklärung genannt und überlegt worden. Dieses sind:

- PIN (know)
- Passwort (know)
- Unterschrift (know/be)
- Fingerabdruck (be)

PIN und *Passwort* sind im elektronischen Geldtransfer die bisher gebräuchlichsten und wären entsprechend einfach umzusetzen. Als Problem stellte sich bei diesen beiden Lösungen jedoch die Nutzbarkeit in den einzelnen „Lebenslagen“. So könnte es einerseits zu später Stunde schwerer fallen einen PIN oder ein Passwort korrekt in einen PDA einzugeben, andererseits könnte es vorkommen daß der Gast die jeweils betätigten Tasten verbal wiederholt und ein dritter so schnell die Zugangsdaten zum eigenen Konto erhalten könnte.

Die *Unterschrift* hingegen würde vermutlich nicht in der vollen Pracht verwendet werden. Vielmehr würde aus ihr eine Signatur abgeleitet werden, die letztendlich als „Passwort“ Verwendung finden würde. Hierbei jedoch bliebe die Frage offen ob bei der Abgabe einer Unterschrift (auf dem PDA) eine Prüfung dieser per Software den nötigen Erfolg bringen würde, zumal bei der Betrachtung herkömmlicher Bezahlverfahren (hier: Lastschrift) auffällt, daß hier nur eine grobe Kontrolle der Unterschrift mit der Musterunterschrift auf der Kreditkarte erfolgt und höchstens bei Problemen mit einer Lastschrift die Unterschrift auf dem entsprechenden Quittungsabschnitt genauer kontrolliert wird. Somit dürfte es bei der Verwendung einer Unterschrift zur Authentifizierung höchstens zu einer groben vorab Kontrolle durch tolerante Software kommen, wonach die Unterschrift als Grafik in einem geschützten Bereich mit Verweis auf die zugehörige Transaktion abgelegt wird.

Abschließend soll hier noch kurz auf die mögliche Nutzung biometrischer Daten zur Authentifizierung eingegangen werden. So bietet z.B. der „HP iPAQ Pocket PC H5550“ die Nutzung eines integrierten Fingerabdruckscanner an, wobei ebenfalls API's von HP zur Verfügung gestellt werden, mit deren Hilfe dieser Fingerabdruckscanner für eigene Funktionen genutzt werden kann.

Bisher nicht berücksichtigt wurden *have*-Schlüssel. Ein solcher Schlüssel wäre z.B. der PDA des Gastes selbst, da er zur Vollendung einer Transaktion benötigt wird. Bei einem vereinfachten System könnte es beispielsweise auch genügen wenn der Gast eine Transaktion per Klick auf einen OK-Button bestätigt, da er sich bereits über einen *Schlüssel* an seinem PDA angemeldet hat und somit seine Berechtigung bereits nachgewiesen ist.

Bezahlen Sie doch einfach mit Ihrem „guten Daumen“
- Bei EDEKA per Fingerabdruck bezahlen -

Wie erst vor kurzem von der EDEKA Handelsgesellschaft als Testprojekt A.1 auf die Welt gebracht, könnte dem Gast bei diesem Projekt die Möglichkeit gegeben werden, an den Kassen direkt mit seinem „guten Daumen“ zu zahlen. So könnte er mit Hilfe des PDA's sein Konto verwalten, sowie ausgewählte Transaktionen direkt buchen, bräuchte jedoch den PDA nicht am Abend mit in die Disco nehmen, da er hier per Fingerabdruck sicher zahlen kann.

4. Ein erster Entwurf

4.1. Die architektonische Darstellung

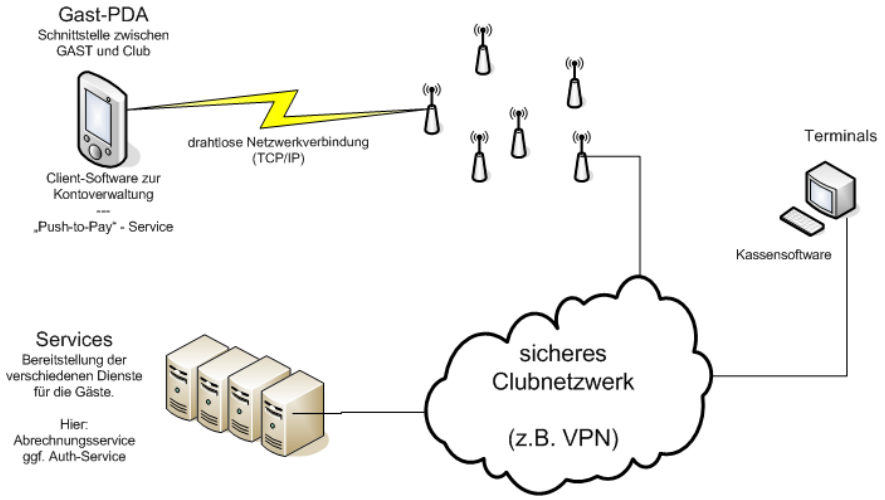

Abbildung 4.1.: architektonisches BigPicture - Grobriß des entstandenen Systems

Diese Skizze soll abschließend einen möglichen Aufbau des für die Realisierung benötigten Netzwerkes darstellen.
Dabei soll herausgestellt werden, daß ein Ferienclub-Gast ein mobiles Gerät (hier einen PDA) während seines Aufenthaltes zur Verfügung hat, mit dessen Hilfe er bestimmte Dienste in seinem Ferienclub nutzen kann. In diesem Fall soll der PDA die Funktionen einer Geldbörse bzw. einer Kreditkarte übernehmen.
Weiterhin soll aufgezeigt werden, daß dieses System aus insgesamt drei Hauptkomponenten besteht:

- PDA - mit dessen Hilfe der Gast Zahlungen im Club vornehmen kann
- Server - welche die benötigten Services bereitstellen (Abrechnungsservice/Kontoverwaltung, Authentifizierungsservice)
- Terminals - die als Kassen fungieren und die Bezahlvorgänge starten

Die an die Gäste ausgegebenen PDA's stellen dem Gast den Zugriff auf das eigene Konto zur Verfügung, wodurch der Gast jederzeit, sofern er in der Reichweite des Clubnetzwerkes ist, z.B. sein Guthaben bzw. die einzelnen Umsätze eines Zeitraumes überprüfen oder Guthaben an andere Clubgäste transferieren kann.
Zusätzlich bieten diese PDA's dem Gast eine zentrale Stelle, an der er Transaktionen bestätigen kann, sofern diese durch einen Service gefordert werden, ohne daß er sich zu bestimmten Terminals begeben muß.

Die Server hingegen stellen, wie genannt, die Services bereit auf die die PDA's und Terminals zugreifen.
So werden letztlich alle Transaktionen durch den Abrechnungsservice durchgeführt, wobei die Initiierung einer Transaktion durch ein Terminal oder einen PDA erfolgt und ggf. die Anforderung einer Transaktionsbestätigung durch den zu belastenden Gast bei dessen PDA angefordert wird.

Die Terminals bieten eine grob angepasste Funktionsweise der PDA-Software, da hier anders als bei den PDA's z.B. Kassenabschlüsse von nöten sein könnten.

Die gesamte Netzwerkbasis soll an dieser Stelle vorerst unbehandelt bleiben, da sie relativ unabhängig von der finalen Realisierung ist. So könnte in der Regel jederzeit von WLAN zu Bluetooth gewechselt werden oder es könnte ein VPN eingerichtet werden.

4.2. Ablauf-Darstellung des entstandenen Systems

Zusammenfassend soll an dieser Stelle noch einmal beschrieben werden wie die Nutzung des entwickelten eCredit-Systems im Einsatz aussehen könnte.

Die Ankunft

Bei der Ankunft im Club wird der Gast wie bisher eingecheckt.
Im Anschluss an diese Prozedur erhält der Gast einen PDA ausgehändigt und wird in die Nutzung des Gerätes eingewiesen.
Zusätzlich erfolgt die Personalisierung des PDA wobei ein Authentifizierungscode (siehe 3.3) auf dem PDA sowie ggf. im Clubnetzwerk eingerichtet wird.
Außerdem wird im Clubnetzwerk eine Zuordnung von PDA -> Gast hinterlegt, wodurch die Software später erkennen kann, an welchen PDA Informationen gesendet werden müssen, um diese einem bestimmten Gast zur Verfügung zu stellen.

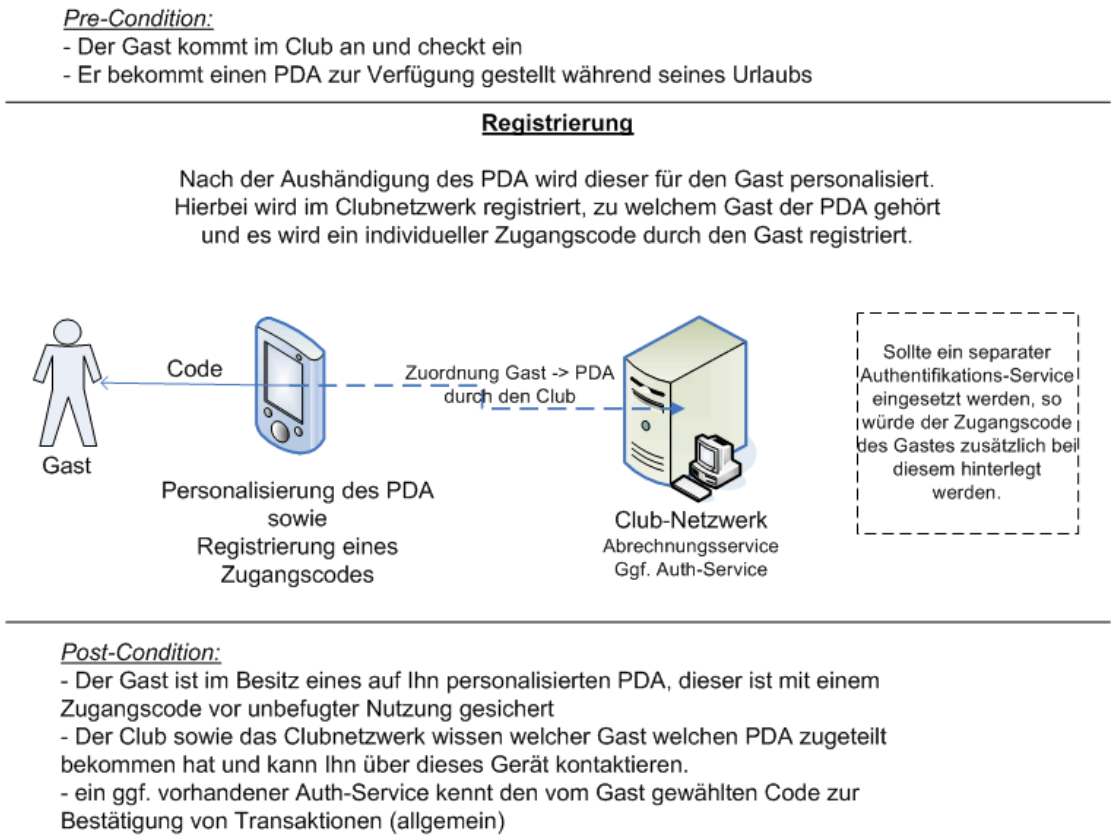

Abbildung 4.2.: Registrierung bei eCredit

Einzahlungen

Zur Einzahlung eines beliebigen Betrages auf ein Gastkonto übergibt der Gast den entsprechenden Betrag an einen autorisierten Club-Mitarbeiter (z.B. an der Rezeption oder Information). Dieser startet eine entsprechende Transaktion, wobei der Betrag sowie der empfangende Gast vom Abrechnungsservice registriert werden und der entsprechende Betrag auf dem eWallet-Konto (auf dem PDA) des Gastes gutgeschrieben wird.
Die Gutschrift des Betrages kann der Gast im Anschluss an die Transaktion über die Client-Software auf seinem PDA kontrollieren.

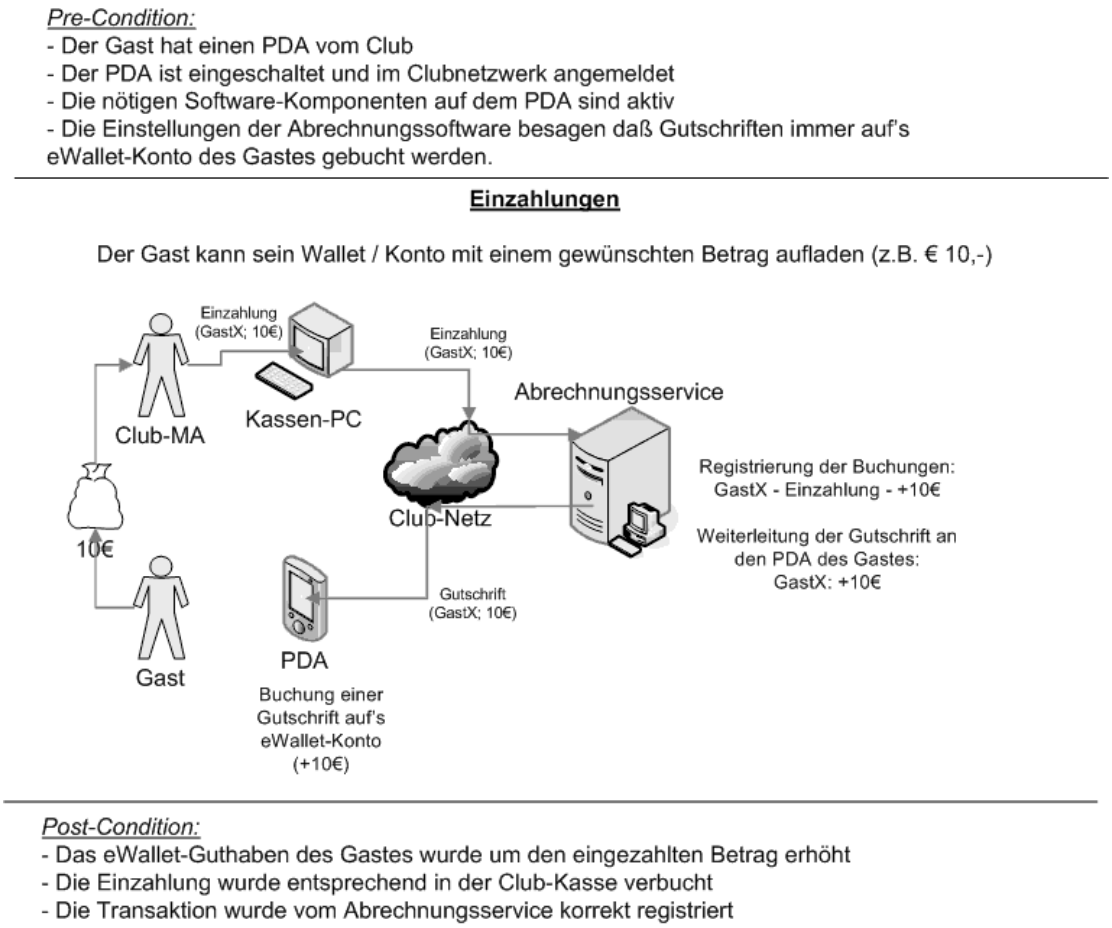

Abbildung 4.3.: Einzahlungen bei eCredit

Kontoabfragen

Für eine Abfrage der durchgeführten Transaktionen benötigt der Gast nur bedingt eine Verbindung zum Clubnetzwerk.
Sollte keine Verbindung zum Clubnetzwerk bestehen, so kann der Gast nur die Kontoinformationen (Kontostand, Umsätze, etc.) abfragen, welche in seinem PDA gespeichert sind.
Während eine Verbindung zum Clubnetzwerk besteht, kann der Gast zusätzlich auf die auf dem Server gespeicherten Daten zugreifen und so eine komplette Aufstellung seines Kontos einsehen und prüfen. So kann er in diesem Falle eine detaillierte Aufstellung betrachten, auf welcher Kontoart (eWallet oder eCash) welche Transaktionen verbucht wurden.
Ebenfalls kann der Gast in diesem Fall die Salden der einzelnen Konten betrachten und einen Saldo über alle Konten berechnen lassen, anhand dessen er den gesamt Stand seines Guthabens bzw. Kredites erkennen kann.

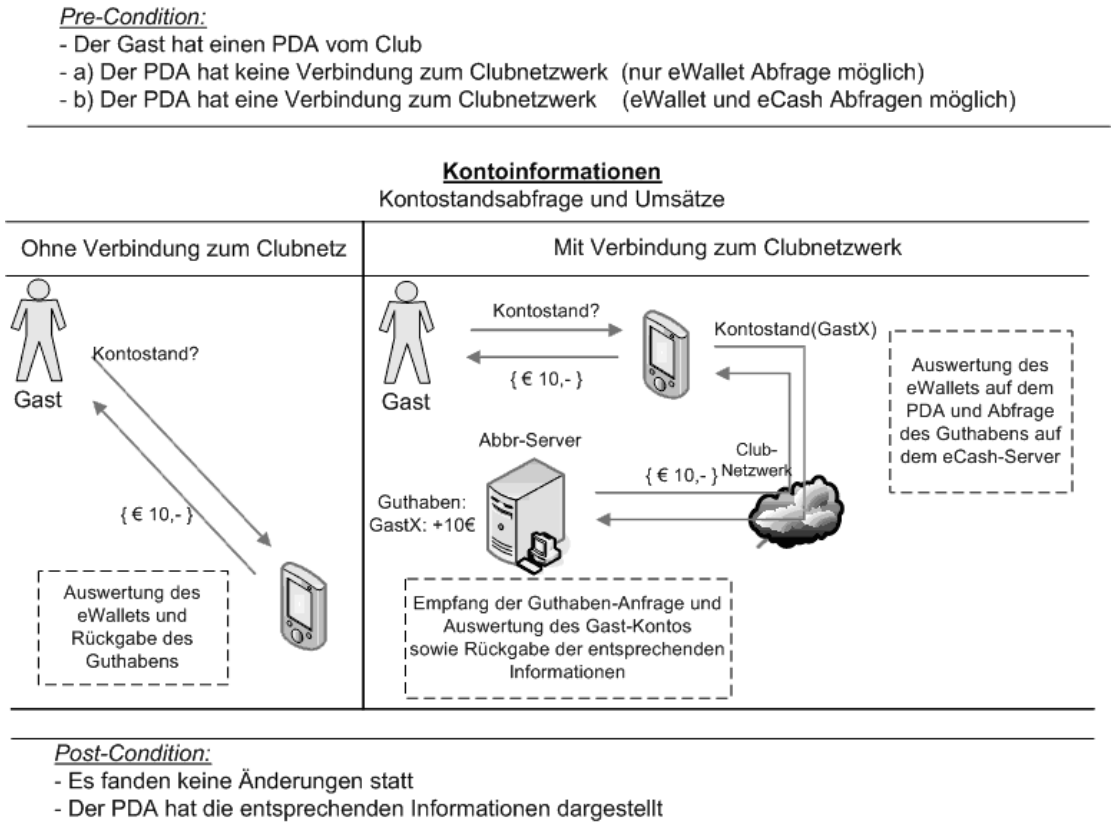

Abbildung 4.4.: Kontostands- und Umsatzabfragen bei eCredit

Transaktionen

Die Transaktionen hingegen stellen einen Sonderfall dar, da ein Gast in der Regel jeweils die Wahl hat ob ein Betrag von seinem eWallet- oder eCash-Konto abgebucht werden soll.

Zur Vereinfachung wollen wir an dieser Stelle davon ausgehen, daß zuerst ein Guthaben auf dem eWallet-Konto aufgebraucht wird, bevor das eCash-Konto belastet wird.

In jedem Fall wird eine Transaktion vom Abrechnungsservice verarbeitet und zum Abschluss eine Freigabe des Gastes eingeholt. Bei dieser Freigabe schickt der PDA einen entsprechenden Betrag aus dem eWallet-Konto des Gastes an den Abrechnungsservice zurück. Sollte das eWallet-Guthaben zur Zahlung ausreichen, so würde der Abrechnungsservice damit die Transaktion abschließen. Fehlt jedoch noch ein Teilbetrag zur Begleichung der Transaktion, würde dieser Fehlbetrag vom eCash-Konto des Kunden abgebucht werden.

Als spätere Erweiterung könnte dem Gast bei der Bestätigung einer Transaktion die Auswahl geboten werden, über welches Konto der zu zahlende Betrag abgerechnet werden soll.

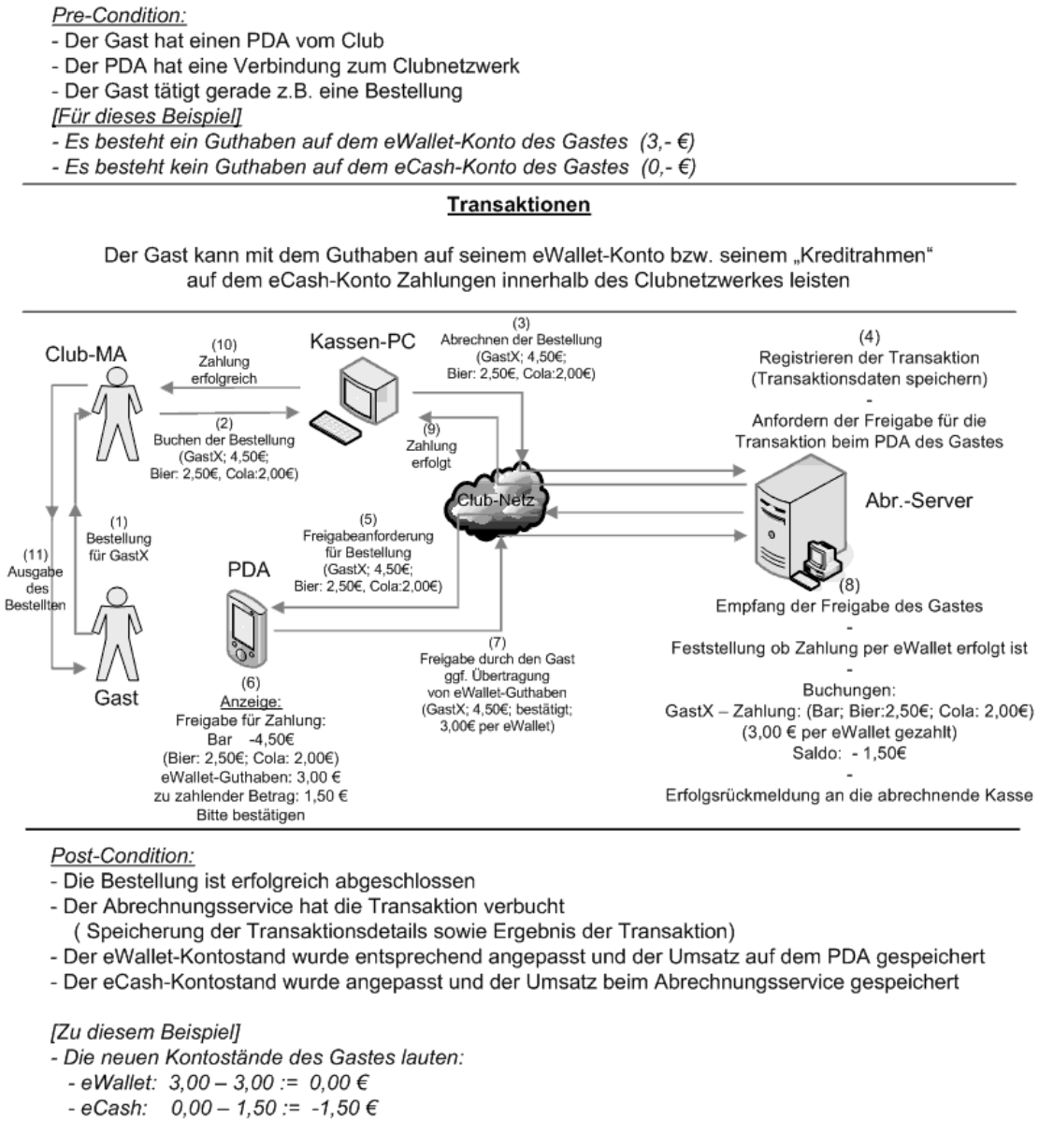

Abbildung 4.5.: Transaktionen bei eCredit

4.3. Ein kurzer Abschluss

In dieser Studienarbeit sollte dargestellt werden in welchem Umfang ein ePaymentsystem mit Unterstütung von PDA's realisiert werden kann. Hierzu wurden bestehende und bekannte Systeme beschrieben und zu einem neuen System zusammengestellt, wobei dieses neue System nur einen erster Entwurf darstellt. In wieweit dieses System in die Realität umgesetzt werden kann, wird in meiner kommenden Diplomarbeit zu diesem Thema nachvollziehbar sein.

A. Anhang

A.1. Referenzen

Allgemein

Thema Bluetooth: http://de.wikipedia.org/wiki/Bluetooth

Zum Thema: Netzwerk und Sicherheit

R.Bartnik - 23.März 2005
Sicheres Wlan im Ferienclub
Studienarbeit - HAW Hamburg - Fachbereich Informatik und Elektrotechnik

A.Lüpke - 20.April 2004
Entwurf einer Sicherheitsarchitektur für den Einsatz mobiler Endgeräte
Diplomarbeit - HAW Hamburg - Fachbereich Informatik und Elektrotechnik

P.Wendt - 11.Juni 2004
Entwicklung CORBA-basierter Middleware für mobile Anwendungen
Diplomarbeit - HAW Hamburg - Fachbereich Informatik und Elektrotechnik

Diese drei vorgestellten Arbeiten sind nachzulesen unter:
http://users.informatik.haw-hamburg.de/ ubicomp/papers.html
Stand: 13.April 2005

Zum Thema: Bezahlen per Fingerabdruck bei EDEKA

heise online - März 2005
EDEKA setzt auf Fingerabdruck-Bezahlsystem
URL: http://www.heise.de/newsticker/meldung/57055
letzter Zugriff: 13.04.2005

Stern Shortnews - März 2005
EDEKA - Fingerabdruck als Zahlungsmittel
URL: http://shortnews.stern.de/shownews.cfm?id=562674
letzter Zugriff: 13.04.2005

T-Online Business-Themen - März 2005
Mit dem Finger an der Kasse
URL: http://www.t-online-business.de/c/36/71/05/3671056.html
letzter Zugriff: 13.04.2005

Versicherung über Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Arbeit im Sinne der Prüfungsordnung nach §24(5) ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 28. April 2005	
Ort, Datum	Unterschrift