Portal Payment Possibilities

for a start-up company

Master of Science thesis
2000-12-13

Fredrik Jansson
e95_fja@e.kth.se

Marcus Larsson
e95_mla@e.kth.se

Assignor:	Department of Teleinformatics, Royal Institute of Technology.
Examiner:	Professor Gerald Q. Maguire Jr.
Supervisor:	Andreas Zetterberg, Fredrik Söderberg.
Benefactor:	Celltribe Business Solutions AB.

Abstract

The corporate climate for start-up companies in Sweden has been extremely good for the last couple of years. A lot of small companies have been entering the Internet business arena in different areas such as consulting, content providing, and system developing. Especially the mobile fraction of the Internet field is today a hot topic in Scandinavia and it is rapidly spreading to the rest of the world.

This Master of Science thesis investigates how a small start-up company operating in the mobile Internet field could be able to let its customers pay for the companies services.

Different payment possibilities have been described, compared and evaluated. Amongst the possible solutions are direct Internet payment, credit cards, and micro payment systems. The evaluated solutions are mainly focused on enabling Internet based payments to take place, but the goal is to be able to conduct payments using a standard mobile device.

Several technologies could be used to extend the Internet solution to the mobile market. Techniques that can be used and are evaluated in this thesis are: CTI, SMS, WAP, and SAT.

When offering payment possibilities on the Internet an obvious problem is the security matters. Nevertheless this thesis describes and evaluates the possible solutions available today and a large factor when extending the Internet based payment method to the mobile area are the user confidence and easy to use factors. Furthermore the chosen solution should be possible for a small company to implement. That means that no hardware implementations in the mobile device are acceptable.

Two possible solutions have been implemented and are described in the report. First a real credit card solution for the web case. Second the web solution has been extended to work in a wireless GSM environment using SMS.

Preface

We have been working on this Master of Science thesis from June 2000 to December 2000. The work has been conducted at Celltribe Business Solutions AB in Stockholm, Sweden, for the Department of Teleinformatics at the Royal Institute of Technology – KTH.

Celltribe Business Solutions is a European provider of solutions in the field of mobile communication. They develop and implement mobile strategies and provide mobile services that promote the business and the efficiency of their clients.

Thanks to our industrial supervisors Andreas Zetterberg and Fredrik Söderberg at Celltribe Business Solutions AB and to our advisor at KTH, Professor Gerald Q. Maguire Jr.

Below are two quotations, which give a good reflection of the whole Master of Science thesis project:

You have a lot to learn.
Michael Peterson

Things Take Time.
S3, KTH

This is Celltribe

The possibilities in the mobile revolution are immense. Celltribe's objective is to make those possibilities available for their clients.

Celltribe Business Solutions (CBS) is a European provider of solutions in the field of mobile communication. They develop and implement mobile strategies and provide mobile services that promote the business and the efficiency of their clients.

Celltribe Business Solutions' objective is to build mobile platforms around tried and tested technologies that work - SMS Network. More specifically, they are building communication solutions for mobile telephones, WAP telephones, Nokia Communicators and PDAs. Celltribe is offering secure connections to systems such as ERP, MIS, CRM, Sales Support, Intranet, MS ExchangeTM, Lotus NotesTM, etc.

CBS services range over the following areas:

- Mobile strategy.
- Mobile marketing.
- Mobile business support.

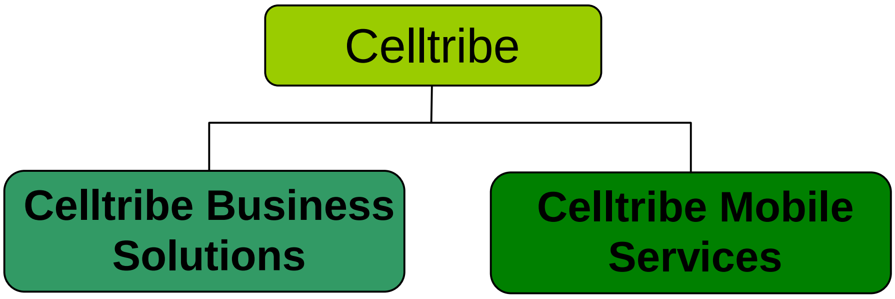
Within these areas CBS operate as a total supplier, offering services ranging from strategic development in the field of mobile IT to the implementation and hosting of new technology.

Celltribe Business Solutions is a company in The Celltribe Group. Celltribe is a group of companies with the joint mission to empower end-users with superior mobile services wherever they are, regardless of time and space.

The Celltribe Group was founded 1999 and at the present they run operations in Sweden, England, and Spain. The Celltribe Group currently employs 90 people. The head office is situated in the city of Stockholm.

Beside CBS a main part of the Celltribe Group is Celltribe Mobile Services (CMS). They are running a portal on the Internet (http://www.celltribe.se). On the Internet site the customer can choose to subscribe to several different services. The information is delivered to the mobile phone via SMS on a regular basis. Some services have a useful approach, such as stock watching, while others are just for fun. Typical examples of the later type of services are horoscopes and cocktail tips.

At the present moment the services do not cost any money, only points. In this report these points are called CellPoints. This term is not an official name since Cellpoint is a company working in the field of positioning.



The Celltribe group.

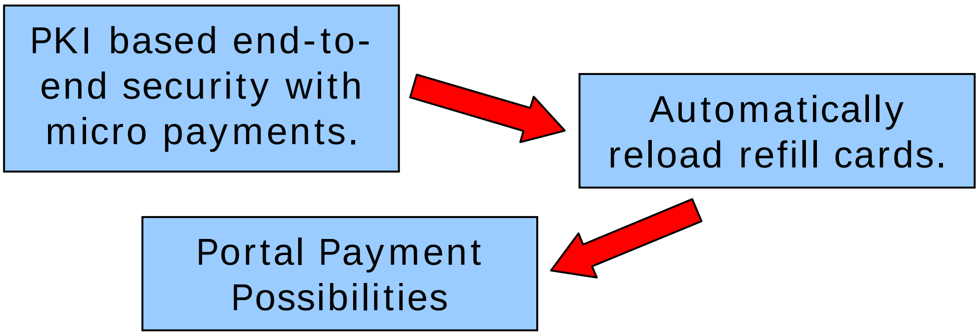
Progress of our work

We started out our thesis work by trying to achieve a secure connection between a mobile device and an application server on the fixed Internet. After investigating a lot of various alternatives presented by different companies in the security area, the conclusion was that a working solution in some way involved changes or reprogramming of hardware. Because Celltribe is a rather small actor on the mobile market and therefore has very small possibilities to influence the large phone manufacturers and network operators, constructing such a solution was not in the company's interest.

Therefore, the priorities changed and we started to look at how Celltribe, in a smart way, could reload their customers' mobile phone refill cards. This includes charging the customer for the reload purchase. However, there are fast changing in priorities in the mobile arena, and Celltribe decided that this service should not be developed internally in the company but rather as collaboration with other portals.

Once again the main focus of the thesis work was changed. Now we were looking into the possibilities for Celltribe to charge for their mobile services, which so far has been free for the customer to use. We used their existing loyalty point system and implemented a working solution on how to charge the users.

Because of the numerous change in priorities described above, the report consists of some material from all three objectives.


PKI based end-to-end security with micro payments.
Automatically reload refill cards.
Portal Payment Possibilities

Progress of our work.

Organization and Coverage

Chapter 1: Cryptography and Security
Describes different techniques, algorithms, and protocols related to cryptography and security. If you possess basic knowledge in the field of security, it is not essential for the understanding of the report to read this chapter. Some sections of this chapter can be rather deep and is preferable used as reference to the rest of the report.

Chapter 2: Security Related Companies
This chapter is a market research of existing security related companies, and briefly describes their business and products.

Chapter 3: Electronic Currency
This chapter describes what electronic currencies really is and also looks a little deeper into some existing ones.

Chapter 4: Mobile commerce
Gives a background to the discussion about the future forecast of the mobile Internet. It deals with the mobile and Internet growth, services and common business development.

Chapter 5: Payment methods
This chapter describes different kinds of payment methods and solutions. The solutions mentioned are mainly focusing on the Swedish market.

Chapter 6: M-commerce enabling technologies
Describes some different communication technologies, which has a possibility to be used as a bearer of m-commerce transactions. Technologies that are examined are WAP, SAT, SmartCards, GSM, GPRS, and CTI.

Chapter 7: CellTribe's Competitors
This chapter looks at some of Celltribe's nearest competitors, investigating if they are using any payment system and in that case how they have solved the payments.

Chapter 8: Demand for Mobile Internet
This chapter tries to motivate why a start-up company like Celltribe acting in the mobile field should introduce some kind of own constructed cyber currency.

Chapter 9: Evaluation of existing payment methods
This chapter tries to motivate what kind of payment method or system is the best to use in Celltribe's specific case.

Chapter 10: Potential mobile payment enabling technologies
This chapter briefly describes some different potential payment technologies, which can possible be used in the Celltribe case.

Chapter 11: Mobile payment solutions – a comparison
Describes and compares three different ways of mobile communication, which can be used for and implemented by a start-up company like Celltribe, to help them expand their payment possibilities to the mobile market.

Chapter 12: Implementation of payment solutions
Describes two live and working implementations, which we have developed to enable Celltribe's portal customers to buy more CellPoints using their credit cards. The first

implementation can be reached using regular Internet web pages. The second one is extended to the mobile phone, using a kind of interactive SMSs to handle the communication.

Chapter 13: Future work

This thesis describes the payment solutions available for a start-up company to implement today. However there exist some aspects that would be interesting to follow up. This section describes some of the enhancements that could be interesting to investigate in the area of portal payment possibilities.

Contents

1 Cryptography and Security

If you possess basic knowledge in the field of security, it is not essential for the understanding of the report to read this chapter. Some sections of this chapter can be rather deep and is preferable used as reference to the rest of the report.

Although the word cryptography can be considered to be relatively well known most people would not be able to explain the meaning of cryptography if they were asked to describe it.

What cryptography is can be rather difficult to define. Simply put, cryptography can be described as the discipline of being able to cloak private material from all other parties than the intended receiver. That means that communication in any form should be kept safe from all entities other than the sender and the receiver. More technically speaking the meaning of cryptography can be defined as the study of techniques and applications that depend on the existence of difficult problems, for example "hard mathematical problems". These mathematical problems can be hard to solve because their solutions require some unknown knowledge or simply because they require much computer power (i.e. time) to break. If for example the secrets are changed every day there is often little meaning in trying to break them if it on average takes two days to find the secrets.

Two related concepts that can be considered to have really tight connections to cryptography are cryptanalysis and cryptology. The first is the analysis of how to crack codes, decode secrets, violate authentication schemes, and in general, breaking cryptographic protocols. Cryptology is the area that combines the two fields of cryptography and cryptanalysis. [1]

1.1 Encryption and decryption

Two really important concepts when discussing cryptography are encryption and decryption. Encryption is the action when the original data is transformed into something that looks and is completely incomprehensible to anyone lacking the correct knowledge of how to interpret the message into the original data. Encryption is used to guarantee that even if a third party gets possession of the data it is impossible for the interceptor to understand the meaning of it. Thus the data, possibly holding important information, is confidential for all except those whom the data was intended for.

Decryption is simply the opposite of encryption. Given the correct information of how to interpret the received data it is possible for the receiver to transform the received (encrypted) data back to its original form.

The technique of performing encryption and decryption require some kind of secret information shared by the two entities sending and receiving the data. This secret can be of various forms and is described later. An important aspect of these secrets, often described as keys, are their distribution, i.e. getting them to the sender and the receiver.

1.2 Authentication

Today's cryptography is more than encryption and decryption. A concept just as important as encryption/decryption (mentioned above) is authentication. Authentication is of great importance because without it one does not know who sent the original data. The authentication is most often achieved using some kind of secret in combination with some predefined algorithm which together produces a hash or digest that can only be calculated by the two entities that hold the correct secret.

1.3 Techniques in cryptography

Today there exist two different types of cryptographic systems that work in slightly different ways. These systems are referred to as symmetric cryptography (using symmetric ciphers) and asymmetric cryptography (using asymmetric ciphers) and are described in the following sections.

1.3.1 Symmetric cryptography

This is the classical sort of cryptography and can be divided in two classes; block ciphers and streams ciphers. In this kind of cryptography the exact same secret key is used both for encryption and decryption. Therefore the algorithms used in symmetric cryptography often are referred to as secret key algorithms. Before sending any data between two participants both entities have to agree on which algorithm they will use and they must also ensure that they are using the same secret key, otherwise nothing will work. After agreed on these the sender encrypts the data with the secret key and sends it to the receiver that decrypts the data using the identical key.

While this may sound simple at a first glance one soon realises that having this kind of system raises a lot of problem. The distribution of the secret keys has to be performed in some secure way, probably manually and even then a trusted courier has to be found. This is a really negative feature of symmetric cryptographic systems since if an entity in the middle gets hold of the secret key it can understand all the communication between the sender and the receiver.

Furthermore the system has problem with its scalability, as the number of participants rises so does the number of key pairs. Every new participant needs to have a new secret computed for all other entities in the system and therefore every entity in the system needs to be equipped with that new secret. One soon realizes that after a while one will have a very complex system that will be very hard to administer.

Today the most commonly used symmetric cryptographic system is Data Encryption Standard (DES), although more and more organisations today are using a variant of the algorithm that is called 3DES. Both variants are described in 1.12.5.

1.3.1.1 Block ciphers

When using block ciphers the specified algorithm is applied to a fixed sized length of the data that is to be encrypted. As with all other symmetric ciphers it uses a secret key and it results in a block of the same length, but now the data is encrypted.

The technique of the block cipher can then be divided into different modes. Below you find four of the most common modes of operation:

- Electronic Code Book (ECB).
- Cipher Block Chaining (CBC).
- Cipher Feedback (CFB).
- Output Feedback (OFB).

Electronic Code Book
This is the easiest of the four standard modes. It simply takes one block and encrypts it. An advantage with this is that several blocks can be handled in parallel as shown in figure 1.1.

This also causes some cryptographical problems. Since each block is handled individually, two blocks containing the same original data will produce the same encrypted data. By looking at repeated pattern in the data a cryptoanalysist can relatively easy break the cipher.

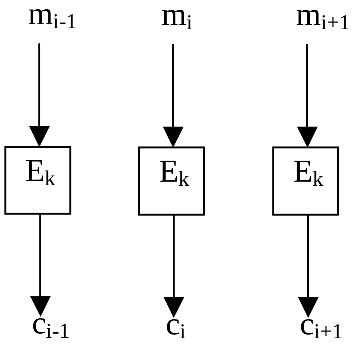


Figure 1.1. The principle of ECB.

Cipher Block Chaining
This mode uses not only the current block but also the previous block in a smart way. The current block is XORed with the previous encrypted one before the current block itself is encrypted (figure 1.2). As a starting value a random initialisation vector, c_0, is used. This initialisation vector is then sent with the message and used during the decryption of the message. This mode makes it impossible to alter the data sent except for the last packages. This results from the fact that every single block is used during the decryption of the original data.

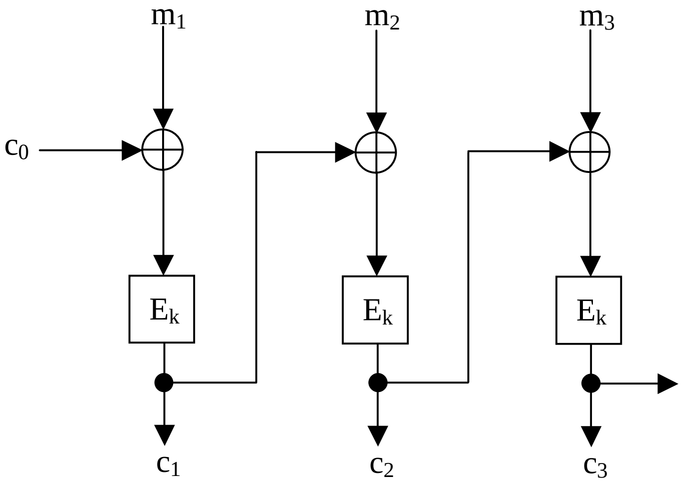


Figure 1.2. The principle of CBC.

Cipher Feedback

This mode is similar to the previous. The difference here is that the current message that is about to be sent is not encrypted. Instead it is the previous block that is encrypted and then XORed with the current message as shown in figure 1.3. Once again a randomly chosen initialisation vector is used to produce unique blocks.

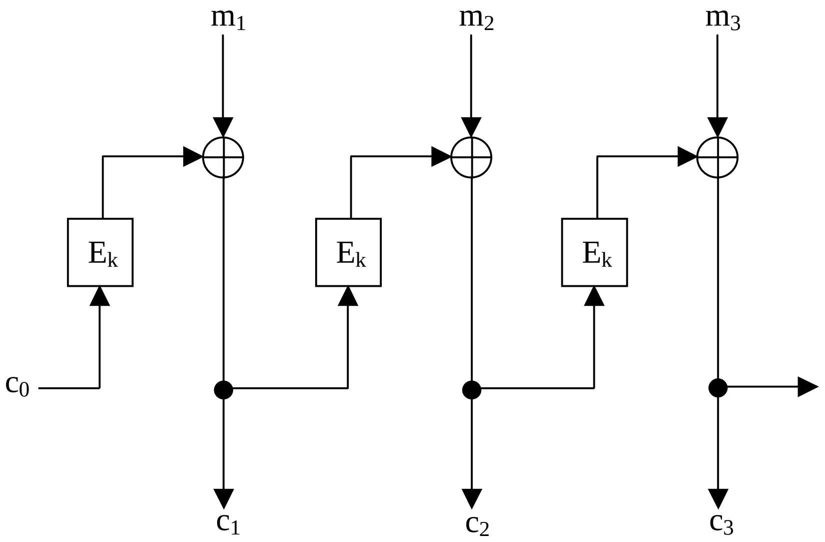


Figure 1.3. The principle of CFB.

Output Feedback

In this mode none of the previous blocks are used when encrypting the current one. Instead an initialisation vector, s_0, is used and encrypted several times. After each encryption the encrypted vector is XORed with the current block.

The principle can be understood by looking at figure 1.4.

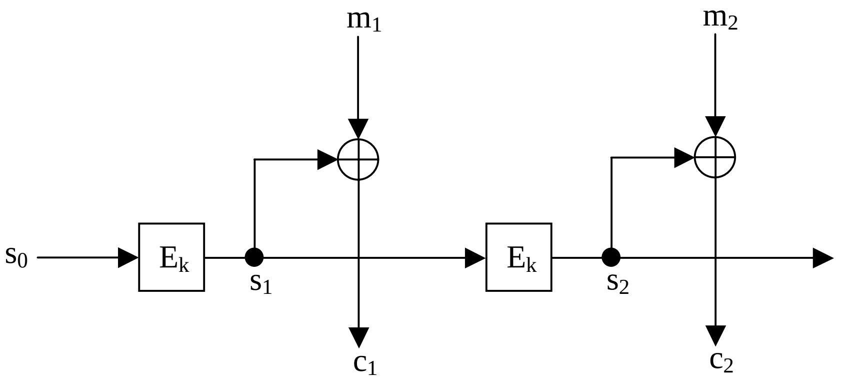


Figure 1.4. The principle of OFB.

It should be noted that this last mode is more resistant to errors during transmission since only the initialisation vector is used during the decryption of all the blocks. Thus a transmission error in one block does not affect the following ones during decryption as it would in the previous two modes.

1.3.1.2 Stream ciphers

Stream ciphers operate on small data blocks, usually not more than a single bit or byte at a time. A stream cipher typically works in the way that it first generates a keystream (i.e. a vector of bits used as a key). Often this keystream depends on some kind of secret key. The keystream is then XORed with the data that is being sent. When the keystream is generated completely independently it is called a synchronous stream and if it is dependent on the data it is called a self-synchronizing keystream. The longer the keystream is the more secure the cipher can be considered to be. This of course raises a lot of key management problems.

Currently there are no stream cipher standards but the most famous one is a cipher called RC5.

1.3.2 Asymmetric cryptography

When using an asymmetric cryptography system both participants need to have one pair of keys each, one public key and one private key. Therefore the algorithms used in asymmetric cryptography often are referred to as public key algorithms. The principle is that each entity will protect its secret key. The public key on the other hand is made public so anyone can obtain it. Normally it will be stored in a public database.

Typically the key pair can be used in two different ways. One approach is that the sender encrypts the data with the receiver's public key. By doing this the sender is sure that only the receiver can decrypt the message using his private key. The other possible approach is that the sender encrypts the data with his own private key. Then the receiver can use the sender's public key to decrypt the message and he knows that the data must have originated from the sender since it is only the sender that could have encrypted the message using his private key.

Obviously these two approaches give rise to some problems. In the first approach the receiver cannot be sure who the sender is because anyone has access to the public key. In the second approach anyone can decrypt the data from the sender because once again everyone has access to its public key.

The solution to these problems is to use a combination of both the sender's private key and the receiver's public key. For example the sender could encrypt the data with the receiver's public key (only the receiver can decrypt it) and then encrypt the already encrypted data with its own private key (now the receiver know that the data must have originated from the sender). As in the case of using symmetric cryptography both parties must be aware of how the transmissions will be decrypted before sending any data between each other, otherwise nothing will work.

The private and the public keys are of course linked mathematically to each other. Due to the fact that the public key is free for anyone to analyse, it is extremely important that it is very difficult to deduce the private key from the public one.

There are several variants of asymmetric algorithms available on the market today. The most commonly used is RSA. With more and more wireless devices operating with a limited bandwidth a new type of cryptographic system called Elliptic Curve Cryptosystems (ECC) have been developed using a new type of algorithm that provides the user with the same security as the old RSA algorithm but with shorter keys. Yet another well-known asymmetric cryptosystem is the Diffie-Hellman key agreement protocol that is often used in collaboration with the Diffie-Hellman algorithm (see section 1.13.4) to derive keys between two entities without having any pre-shared secret.

1.4 Mathematical hard problems

There exist some standard mathematical problems that all successful cryptographic algorithms are based on. These problems are referred to as hard problems not because of their great complexity but rather because of the heavy computational power that is required to solve them. The two standard hard problems are: integer factoring problem and the discrete logarithm problem.

Integer factoring
The factors of a positive integer are the integers that evenly divide it. For example, the divisors of 28 are 1, 2, 4, 7, 14 and 28. When performing a factorisation one is trying to divide the original number into smaller parts (factors). For example the factors of 28 could be 7 and 4 or 2 and 14. A special case of factorisation is prime factorisation where the factors are required to be primes. Multiplying two primes together is easy but it is an extremely difficult problem to invert, i.e. finding the two primes only knowing the result of the multiplication. The RSA algorithm is based on this particular hard problem.

Discrete logarithm
This is the hard problem that for example the well-known Diffie-Hellman algorithm relies on. The principle is that given three numbers; a large prime (*p*), an integer that is smaller than (*p-1*) and a third number (*g*) depending on these two numbers, it is enormously difficult to find another integer, *x*, that fulfils the equation: $y = g^x \bmod p$.

1.5 Perfect Forward Secrecy

Some systems such as the Diffie-Hellman key exchange system use a long-term key (such as the shared secret in IKE[2]) and generate short-term keys periodically. If an attacker who acquires the long-term key provably can neither read previous messages that he may have archived nor read future messages without performing additional successful attacks then the system has Perfect Forward Secrecy (PFS).

The attacker needs the short-term key in order to read the traffic and merely having the long-term key does not allow him to infer these. Of course, it may allow him to conduct another attack (such as man-in-the-middle attack described in section 1.8) which gives him some short-term keys, but he does not automatically get them just by acquiring the long-term key.

1.6 Hash functions

Hash functions are mathematical functions that take a variable length of data and calculate a string with fixed size depending on that data. This value is called a hash value or simply a hash. This value is also sometimes referred to as a message digest. The hash or digest can be said to be a summary or fingerprint of the document since preferably all the data in the original message affect the value of the hash.

The need for hash functions is obvious. It can be used in the following way. The sender calculates the hash and sends it with the original message to the receiver. The receiver then recalculates the hash and compares his value with the sender's value. If they are the same the receiver can be sure that no one has altered the message during the transmission.

There are some important criteria for a hash function that has to be fulfilled in order to make it useful. First of all the function should take an arbitrary amount of data as input but produce a fix length output. Furthermore the function should be rather easy to compute but it must be a one-way function. This means that given the hash it should be impossible (i.e. extremely time consuming) to calculate the original message. The last condition on a high-quality hash function is that two messages should not produce the same hash, if this is fulfilled the hash function is said to be collision-free.

The most widely used hash functions today are SHA-1 and MD5. These are both described later in section 1.13.1 and section 1.13.2.

1.7 Message Authentication Code

In the previous section hash functionality was described and explained. One problem though is if a third entity situated between the sender and the receiver catches the message from the sender, removes the hash, alters the message and then produces a new hash that he appends to the message before sending it on to the receiver. In this case the receiver has no way to see that the message has been altered. The MAC idea can be applied to most cipher techniques such as ordinary hash functions (HMAC), block ciphers and stream ciphers.

The idea with MAC is to use a shared secret when applying the hash function to the message. As in the ordinary case with a hash function a hash is produced but usually it is called a checksum when discussing MAC. In this way no one can alter the content of the message during transmission without the receiver noticing it. On the other hand the shared secret must be distributed between the sender and the receiver in some secure way.

1.8 Types of attacks

There exist a number of terms that can be considered as the basic knowledge to be aware of when doing research or working in the security and cryptographic area. Being aware of these types of attacks makes it easier to avoid being exposed to them. Here follows a list of these concepts.

When discussing the different attacks there are essentially three things one should keep in mind. First the amount of work and computational power the attacker must have access to. Second the amount and type of data that is necessary. Third, one should be aware of the actual value of the data that is being protected against an attacker.

Passive attack
An attack in which the attacker only eavesdrops and attempts to analyse intercepted messages, as opposed to an active attack in which he diverts messages or generates his own.

Active attack
An attack in which the attacker does not merely eavesdrop but takes action to change, delete, reroute, add, forge or divert data. Perhaps the best-known active attack is man-in-the-middle. In general, authentication is a useful defence against active attacks.

Brute-force attack
This is a quite straightforward technique. Just trying every possible key in some logical order until the right key is found. To be able to practice this time consuming technique the attacker must be in possession of both the original message and the encrypted message. In some special cases for example when the original message is in ordinary ASCII characters, then the attacker only needs to have possession of an encrypted text.

The problem with brute-force attacks varies over time. As the computer hardware gets faster and cheaper the use of old algorithms with fixed key length that used to be considered as secure suddenly may be considered as rather insecure.

Birthday attack
This is a usual form of attack against a hash function. A birthday attack is a form of brute-force attack. The attack is based on the birthday paradox (the mathematical fact that in a group of 23 people, the chance of a least one pair having the same birthday is over 50%, as the number of people in the group grows the chance of two people having the same birthday increases surprisingly rapidly)

This mathematical fact turns up whenever the question of two cryptographic operations producing the same result becomes an issue:

- Collisions in message digest functions.
- Identical output blocks from a block cipher.
- Repetition of a challenge in a challenge-response system.

These three items must be avoided in turn to not being exposed to a birthday attack.

Man-in-the-middle attack
A man-in-the-middle attack is categorized as an active attack in which the attacker impersonates each of the legitimate players in a protocol to the other. For example, if the sender and the receiver are negotiating a key via the Diffie-Hellman key agreement scheme, and are not using authentication then an attacker is able to insert himself in the communication path and by this impersonate both players. The man-in-the-middle attack can be avoided using strong authentication algorithms.

Plaintext attack
The simplest single-message attack is the guessed plaintext attack. An attacker sees an encrypted text and guesses that the message might be, for example, ”CellTribe rules" and encrypts this guess with the public key of the recipient and by comparison with the actual encrypted text, the attacker knows whether or not the guess was correct. For

the attacker to be successful using a plaintext attack the messages transmitted must be extremely uniform.

Race attack
This is a rather tedious attack that can only be used against certain kind of systems that sends the password letter by letter (i.e. byte by byte). The attacker monitors the login procedure but right before the user is about to enter the last entry the attacker cuts in and guesses that last entry. The race attack is hardly ever used.

1.9 Key exchange protocol

A key exchange protocol makes it possible for two entities to, without any pre-shared secret, agree on a secret key to be used in their cryptographic system. The most common algorithm used in a key exchange protocol is the Diffie-Hellman algorithm described in section 1.13.4. For example the ISAKMP [3] in IPSec [4] uses this technique.

1.10 Key management

Key management is just as important as the actual cryptographic algorithms. Without the proper administration of the secrets, strong algorithms are of no use. There are several important aspects that must be considered when designing a key management system. For example users with different privileges must be able to obtain a correct key-pair in a secure way and when a private key is lost all others must be notified, so that they do not accept messages authenticated with that key or encrypt messages with the corresponding public key. Furthermore all public keys must be available for the other users in some accessible database.

The lifetime of a key should be limited. This is because an attacker should not get too much material that can be used in cryptanalysis. The longer a key is used the more encrypted material a possible attacker will get. More material in general makes it easier to break an algorithm. The lifetime and the length of the keys often follow hand in hand. Hence using short-term keys mean that the keys can be kept rather short. There is also another advantage in using short-term keys. If an attacker gets possession of this key he can only use it for a finite time before the key is changed once again.

1.11 Secure Socket Layer - SSL

Secure Sockets Layer (SSL) is the Internet security protocol for point-to-point connections. It provides protection against eavesdropping, tampering, and forgery. Clients and servers are able to authenticate each other and to establish a secure link, or "tunnel," across the Internet or Intranets to protect the information transmitted.

In applications using SSL, the confidentiality of information is ensured using strong encryption technologies. Through the use of digital certificates, SSL provides the transparent authentication of servers and, optionally, clients as well. SSL uses the RSA algorithm as the algorithm to enable security using digital signatures and digital enveloping. Other algorithms are available in the SSL specification as well. Based on the strong cryptography in SSL, users have confidence that their information is confidential, authentic, and original during a network connection.

1.12 Public Key Infrastructure

A Public Key Infrastructure (PKI) can be described as a robust framework to secure transactions over public networks. These transactions include anything from exchanging information to buying or selling merchandise and services. [5]

To be a little more specific the term Public Key Infrastructure can be defined as a combination of hardware and software, protocols and procedures. Although different PKI systems can be quite different from each other they are all using the technique with a key pair consisting of a private and a public key. An important aspect of PKI is that asymmetric encryption methods require reliable distribution of the public keys. All participants must be able to be sure that the public keys really belong to those parties they are said to belong to. Therefore the Public Key Infrastructure must include reliable third parties such as Certification Authorities. The primary goal for the infrastructure is to produce reliable security service for the net, regardless of if the infrastructure consists of the Internet or some radio communication network. The most common components of a PKI are:

- Certificate Authority (CA).
- Certificate Revocation List (CRL).

1.12.1 Certificates

A certificate is a digital document that binds a public key to its rightful owner. By using a certificate an entity can ascertain that a specific public key belongs to the correct entity.

Although certificates can contain a lot of different information there are some standard data that it must contain. These are a public key and a name. Other common data that the certificate may contain are expiration date and the signature of the CA.

The leading certificate standard is X.509 [6].

1.12.2 Certification Authority

The Certification Authority can be described as a third party, trusted by everyone. It is at the CA that the public key is stored after it has been generated. When the key is stored the CA hands out a certificate containing that specific public key along with a hierarchy of certificates verifying the CA. Thus the user is able to authenticate the public key.

The CAs are organized in a hierarchal organisation as shown in figure 1.5. Thus a CA can authenticate another CA. This enables different CA’s to authenticate certificates from other CAs as long as the other CA has been approved in advance.

As implied above the CA itself also has a key pair. It is used to assure the correctness of a user's public key. This key pair is extremely important. The private key must be stored in an exceptionally safe place. This is because if the CA's private key is compromised, an attacker will be able to produce fake certificates. Hence all trustworthiness of the CA will vanish. Additionally the public key or the certificate must of course posses a high level of trustworthiness. This can be achieved in two ways. Either the public key or a certificate from a higher level CA must be made available to confirm the correctness of the CA's public key.

The protection of the top CA's key pair is of great importance. If they are compromised the whole hierarchy falls apart.

It is notable that different CAs can offer different levels of trustworthiness. Some CA may issue certificates only based on for example e-mail addresses while others demand the user to identify himself in some physical way. Therefore certificates from different CAs should be valued differently.

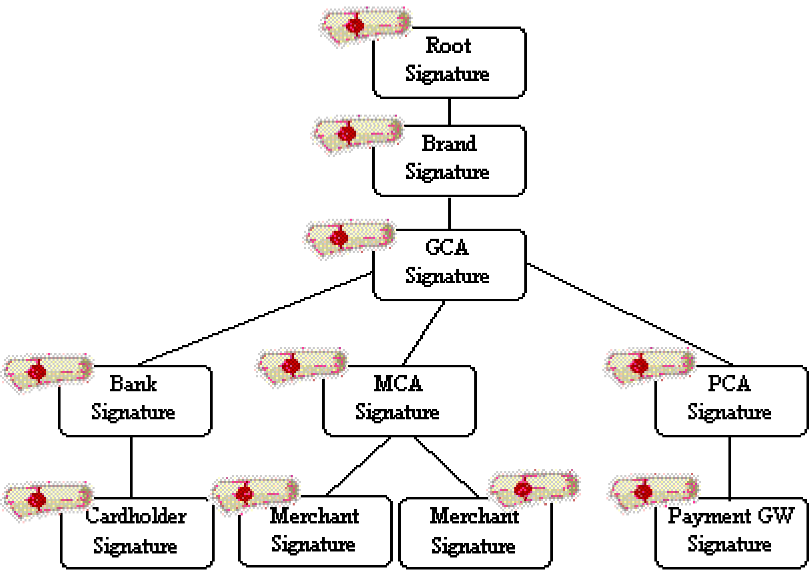


Figure 1.5. Example of a hierarchy of trust.

1.12.3 Certificate Revocation List

The CRL is used to prevent certificates that are no longer legitimate from being used. All revoked certificates are listed on the CA's CRL until they have reached their expiration date. Then they are removed from the CRL since they should not be accepted anyway.

Every PKI system must deal with the possibility that private keys are lost or destroyed. If that happens the CA must be contacted and the corresponding key will be revoked and put on the CRL. This prevents the key from being misused.

The system must also consider that an attacker can compromise the private key. Once again the CA must be contacted immediately and the public key will be revoked and put on the CRL. This prevents the key from being misused.

1.13 Common algorithms

There are a few common algorithms for symmetric and asymmetric encryption that are used in practically every security system.

1.13.1 SHA

The Secure Hash Algorithm (SHA) designed by NIST/NSA, later substituted by the slightly revised SHA-1 is defined in FIPS 180-1 [7]. The hash algorithm can be used to generate a compressed representation of the original message called a message digest. The SHA-1 algorithm uses 80 steps in the process of compressing the original message.

The SHA-1 algorithm operates on blocks with the fixed size of 512 bits. Consequently the total length of a message must always be a multiple of 512 bits. The original message is therefore padded (extended). The padding is done by first adding a 1-bit to the original data. Thereafter follows a number of 0-bits followed by a 64-bit integer that represents the length of the original message. All together the block size should now be a multiple of 512. The message digest is computed using this final padded message. The calculated message digest is a 160 bit long checksum. This checksum is then appended onto the original message before it is transmitted.

Using the SHA-1 algorithm when a message is received then the included checksum is removed from the received message and a new checksum is computed as described above. These two checksums are then compared and if they are the same the receiver can be sure that no one has altered the message and it can be passed on to the next higher level protocol as usual.

1.13.2 MD5

Message Digest 5 (MD5) [8] is the latest hash algorithm designed by Ron Rivest. It was developed in 1992 and as in all hash-like algorithms it produces a compressed representation of the original message called a message-digest. The MD5 algorithm uses a total of 64 steps divided into four rounds. The input message may be of arbitrarily length.

As in the SHA-1 case the original message is padded so the message is a multiple of 512 bits in length, including a 64-bit representation of the length of the original message (before the padding) at the end.

The message has a length that is an exact multiple of 16 and can be divided into 32 bits words. After the padding an initialisation of a buffer is done. This four word buffer (A,B,C,D) is used to store the message digest. Four auxiliary functions are also defined such that each takes as input three 32-bit words and produces as output one 32-bit word. In this way the size of the text is compressed.

The MD5 algorithm operates blockwise, for example in CBC mode described in section 1.3.1.1. The last output of the compression (i.e. the block mode) function is defined to be the hash value of the message. To be more specific the message-digest can be found in the four word buffer. The message-digest value has a fixed size of 128 bits.

1.13.3 AES

The cryptographic field is always evolving and the need for stronger and faster algorithms can never be satisfied. Therefore the National Institute of Standards and Technology (NIST) has started a competition for specifying one or more unclassified, publicly disclosed block cipher encryption algorithm(s) available royalty-free worldwide that is (are) capable of protecting sensitive information. History has shown that the NIST standard often becomes the world's standard, for example that was the case with the DES algorithm. The goal is to define a new Federal Information Processing Standard (FIPS) referred to as the Advanced Encryption Standard (AES). [9]

The competition has been going on since 1997 and in August 1999 NIST announced that the number of candidates had been narrowed down to the five ones listed in figure 1.6.

Algorithm name	**Submitter**
Mars	IBM(represented by Nevenko Zunic)
RC6	RSA Laboratoriets
Rijndael	Joan Daemen, Vincent Rijmen
Serpent	Ross Anderson, Eli Biham, Lars Knudsen
Twofish	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson

Figure 1.6. Candidates to AES.

More information about these algorithms such as the NSA's final report on hardware evaluations, can be found on the NIST homepage (http://csrc.nist.gov/encryption/aes/).

1.13.4 Diffie-Hellman

The Diffie-Hellman protocol is a public-key agreement protocol developed in 1976 by Bailey W. Diffie, Martin E. Hellman and Ralph C. Merkle [10].

The main purpose of the protocol is to enable two parties, without any earlier agreements, to agree upon a shared secret key, which can be used to encrypt further communication between the parties. In the key-negotiation dialogue, the transformation use non-secret operations that are easily performed but extremely difficult to invert. It is infeasible for an eavesdropper to invert the initial transformation to obtain either parties' secret transformations, or duplicate it to obtain the secure cipher key.

How to generate keys
To have the two parties, over an insecure medium, agree on the same secret key the following is done: First, the two hosts have to get two public parameters p and g, which have to have the same value for both hosts. The p value is a prime larger then 1 (one) and the g value, also called the generator, is an integer less than p.

When referring to the key size for the Diffie-Hellman algorithm, what is meant is the length of the prime p in bits. A typical key-length is 1024 bits.

Each host generates its own private number *x*, which is less then *p-1*, and then generates an own public key *y* in the following way: $y = g^x \bmod p$. The public keys are exchanged between the two hosts, which are now able to generate the same secret key *s* using their own and their opponent's public keys: $s = y^x \bmod p$.

Both parties should have generated the same value for *s* because of the following mathematically similarity: $s = \left(g^x \bmod p\right)^{x'} \bmod p = \left(g^{x'} \bmod p\right)^x \bmod p$

The *s* key can now be used as the encryption key used in the communication between the two hosts.

1.13.5 DES and 3DES

Today, the world's most famous and popular block cipher is the Data Encryption Standard (DES), which describes the Data Encryption Algorithm (DEA) [11]. DEA is an improvement of the *Lucifer* algorithm created by IBM, NSA, and NIST. DEA, often called DES, is based on the *Feistel* cipher by Horst Feistel [12]. There are four different modes which are standardized for DES: Electronic Code Bock (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB). For more information about the different modes see section 1.3.1.1.

DES is a symmetric algorithm and has a 64-bit block size where 8 bits are parity bits. In practise a PKI cryptosystem is used to distribute the DES' secret keys. The DES can be used in both encryption/decryption and authentication.

The consensus of the cryptographic community is that DES is not secure, simply because 56-bit keys are vulnerable to exhaustive search. Therefore the triple-DES or 3DES cryptosystem has been developed. The 3DES is exactly the same as the DES except that the data is going through the cipher system three times.

There are some different methods to use when encrypting the data with 3DES. The most common mode is the DES-EDE, where EDE means that the message is first encrypted, then decrypted and then encrypted again. The keys used in this EDE can be all different, all the same or the encryption keys the same but the decryption key independent:

$C = E_{k_3}(D_{k_2}(E_{k_1}(M)))$, where k_i is the key and *M* the message to be encrypted.

If one chooses all keys to have the same value, 3DES is backward compatible with DES, because the first encryption - decryption will have no effect on the message.

Another method of the 3DES is the DES-EEE, which consist of three consecutive encryptions.

1.13.6 DSA and DSS

The Digital Signature Algorithm (DSA) was incorporated as a part of the Digital Signature Standard (DSS) by the National Institute of Standards and Technology (NIST) in May 1994 [13]. The DSA is a public-key technique based algorithm that takes advantage of the discrete logarithm problem. The algorithm can only be used to provide digital signatures and not for encryption. In this algorithm the generation is faster than the verification of the signatures.

DSA makes use of computation of discrete logarithms in certain groups in a finite field *GF(p)* for some prime *p*. A typically key length is 1024 bits, referring to the prime *p*.

1.13.7 Elliptic curve cryptosystem

Using elliptic curve cryptosystems was proposed by Victor Miller [14] and Neal Koblitz [15] independently of each other in 1985. The main thought was to use the group of points on an elliptic curve and use them in already existing discrete logarithmic public-key cryptosystems.

The security in this lies in the difficulty of solving the following mathematical problem: Given two points *G(x,y)* and *Y(x,y)* on an elliptic curve such that *Y=kG*, find the integer *k*. An elliptic curve over a finite field F is the set of solutions of points (x,y)

Elliptic curves are defined over either the integers modulo a prime number $GF(p)$ or over binary polynomials $GF(2^m)$. The curves over $GF(p)$ are of the form $y^2 = x^3 - 3x + b$, where *b* is random. The curves over $GF(2^m)$ are either of the form $y^2 + xy = x^3 + x^2 + b$ or $y^2 + xy = x^3 + ax^2 + 1$, where *b* is random and *a* is 0 (zero) or 1 (one).

The key size is the size of the prime number or binary polynomials in bits. A typical key size is in the range from 160 to 200 bits. Because of the difficulty in computing elliptic curve discrete logarithms, these shorter key sizes can be used to achieve the same security as in other conventional public-key cryptosystems.

1.13.8 RSA cryptosystem

The RSA system is the most widely used public-key cryptosystem today and was developed in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman [16]. The RSA system offers both authentication (digital signatures) and encryption. In professional practice, the RSA system is often used together with other security systems (i.e. 3DES for encryption and MD5 for authentication) to gain the best performance in both speed and security.

The RSA algorithm security technique is based on factoring very large primes.

How to generate keys
The following shows how the algorithm generates the public and private keys: First two large primes, *p* and *q*, are generated. The two primes are then multiplied with each other and the product *n* is called the modulus (*n*=*pq*). When referring to the key size of RSA, what is meant is the length of the modulus in bits. The most common key size for RSA is 1024 bits. After the computation of *n* a number *e* (the public exponent) is chosen that has to be less then *n* and also has to be a relatively prime to (*p-1*)(*q-1*), which means that *e* and (*p*-1)(*q*-1) have no common factors except 1. Another number *d* (the private exponent) is then chosen such that (*ed-1*) is divisible by (*p-1*)(*q-1*). The public and private keys are now ready and consist of both the modulus and the public respectively the private exponent, *pubkey*=(*n*,*e*) and *privkey*=(*n*,*d*).

Encryption and authentication
To encrypt a message *m* to be sent from one host to another the sending host computes a cipher text *c* to send, using the receiving host's public key (*n*,*e*) : $c = m^e \bmod n$. For the receiver to decrypt the message *c* back into *m* it has to use its own private key

(*n*,*d*): $m = c^d \bmod n$. Because of the relationship between the receiving host's public and private key (*e* and *d*) it is ensured that the decrypted message is correct.

To send a message *m* to a receiving host and be assured that the message is authentic and really sent from the origin host, a digital signature *s* is created at the sending host: $s = m^d \bmod n$, where *d* and *n* are the sender's private key. The signature is then attached to the original message *m* to the receiver. The receiver uses the sender's public key (*n*,*e*) to confirm that the message *m* received is correct: $m = s^e \bmod n$.

Speed
Entire groups of users often use the same public exponent but different modulus in their public keys. It is also common to select a small public exponent (i.e. 3 or $2^{16}+1$ are frequently used numbers). Having a small public exponent will lead to faster encryption than decryption and faster verification than signing.

In a typical implementation of the RSA algorithm, the public key operations take $O(k^2)$ (*O*=*Order*) steps, private key operations takes $O(k^3)$ steps and key generation takes $O(k^4)$ steps. The *k* corresponds to the number of bits in the modulus.

1.14 Comparison of public-key systems

To be able to compare the different algorithms with each other in a realistic way, the key sizes for which the security level in the different algorithms are the same have to be found.

If the RSA algorithm with a key length of 1024 bits acts as the base for this comparison, one can try to determine what DSA, Diffie-Hellman, and elliptic curve key sizes give the same level of security as the RSA-1024.

RSA, Diffie-Hellman, and DSA are all very alike and can therefore easily be compared. The General Number Field Sieve (GNFS) requires almost the same run-time to factor a 1024-bit long RSA modulus as to perform a discrete logarithm with a 1024-bit long Diffie-Hellman or DSA modulus. Therefore all these three algorithms can use a key length of 1024 bits.

When comparing RSA to the elliptic curve variants, it requires a bit more analysis. According to A. Odlyzko using GNFS to factoring a 1024-bit RSA key would require 3×10^{11} MIPS-year. The speed of a normal PC can be estimated by 300 MIP, which will lead to approximately 2^{30} PC-years to factor the 1024-bit RSA key.

The best way to attack the elliptic curve algorithm is to use a parallel collision search. It requires about $2^{k/2}$ elliptic curve additions, where *k* means the multiplier in bits. Using software on a PC the attack time would be approximately $2^{k/2-39}$ PC-years if each elliptic curve addition would be estimated to 2^{-39} years. To compare the elliptic curve with the RSA algorithm the *k* can be chosen to 138 bits ($2^{138/2-39} = 2^{30}$). Because calculating this parallel collision search needs very little memory, it is ideal to be performed in hardware. To be able to achieve the same level of security as for RSA the multiplier's *k* has to be 170 bits long, which requires elliptic curve size of 171-180 bits. This is for the case when using elliptic curves over $GF(2^m)$. Using elliptic curves over $GF(p)$ is about 8 to 10 bits lower because it is more expansive to implement in hardware.

Now the key sizes for the algorithms have been determined and a comparison of speed can be performed. The numbers in the table below are milliseconds on a 200 MHz PC for signing, verifying, key and parameter generation. The values should only be used in comparison with each other, because they can vary a lot between different computers with different speed etc.

	RSA-1024 (e=3)	**DSA-1024**	**Elliptic Curve DSA-168 (over GF(p))**
Signing	43	7	5
Verifying	0.6	27	19
Key generation	1100	7	7
Parameter generation	None	6500	N/A (large though)

Figure 1.7. Comparison of algorithms, times in milliseconds.

It is quite easy to draw conclusions from this table, though the values vary a lot between different algorithms when performing different cryptographic functions.

The most frequently used cryptographic functions are signing and verifying signatures. It can easily be seen that RSA is much faster in verifying then the DSA and the elliptic curve, but a bit slower when it comes to signing the signatures. The DSA and the elliptic curve are very much alike, both in verifying and in signing.

When comparing the encryption and decryption times of the algorithms, it is acceptable to say that it is similar to the signature comparison. Therefore the DSA and the elliptic curve algorithms are alike, but RSA is much faster in encrypting and slower in decrypting.

For on-line key exchange offering PFS, RSA is much slower then the other two algorithms due to the need to create a one-time RSA key pair.

However, it is hard to say which algorithm is the best. They are all suitable for different kinds of security matters. RSA for instance is very well suited for certificate-based systems, where each certificate is signed only once and verified thousands of times. Looking into on-line communication, RSA either has to give up PFS or has to tolerate slow generation of session key pairs. The Diffie-Hellman or the elliptic curve algorithm is in that case better to use. Using wireless communication, there are a lot of factors that one wants to minimize. For instance the mobile devices have limited battery power and processor capacity. With elliptic curves the key size is much smaller than the other algorithms, which makes EC better to implement in PDAs. [17]

1.15 The security protocol IPSec

A large problem with the ordinary IP protocol is that it offers absolutely no security when sending data packets over the Internet. That means that everyone with the right equipment can in fact determine what you are transferring. With the right knowledge a third party could in fact cut off or insert packets in the communication between two hosts.

This is exactly what the IPSec [18] standard from IETF (Internet Engineering Task Force) is trying to prevent. By using several different protocols it is possible not only to ensure authentication but also encrypt the packets that are sent over the Internet.

IPSec operates on the network layer in the OSI model. Therefore it can protect any protocol running above IP and works on any medium. This means that IPSec can protect a mixture of higher level protocols running over a complex combination of media.

An important concept regarding IPSec usage is the Security Association (SA). In reality that is the secure channel negotiated by the higher levels of an IPSec implementation and used by the lower. Note that SAs are unidirectional, that means that you need a pair of SAs to be able to handle two-way communication. An SA is defined by three things; the destination, the protocol (AH or ESP), and the Security Parameters Index (SPI).

1.15.1 Modes of communication

The IPSec standard supports two different modes, transport and tunnelling. Which mode to choose is mainly a question of where IPSec is implemented.

Tunnel mode
Tunnel mode encapsulates the entire original IP packet to tunnel the packet in a secure communication. The tunnel mode is used when IPSec is used in an internetworking device, typically a firewall or router. In this mode the hosts' entire original packet (including the original IP header) is enclosed in a new packet with ESP/AH headers and then transmitted within an secondary IP-header. This adds another level of security since the original IP addresses cannot be seen by anyone until the packet emerges from the tunnel.

Transport mode
The transport mode is used when the host itself supports AH and ESP. In that case the payload field is just the actual data that the host wants to transmit. This results in only one IP-header in the entire packet. Thus this mode should be used when creating secure channels between two workstations and not two subnets.

1.15.2 Protocols

IPSec consists of three different kind of protocols that handles different security aspects. Combined these protocols form the IPSec standard.

- **Authentication Header (AH).**
  Verifies that the claimed sender originated the packet.
- **Encapsulating Security Payload (ESP).**
  Conceals the content of the packet by using encryption.
- **Internet Key Exchange Protocol (IKE).**
  Handles the exchange of session keys between the hosts that are communicating.

1.15.2.1 Authentication Header

The authentication header is able to cover the whole original packet and offers a connectionless service (i.e. packet by packet service). The header contains several fields; a Security Parameter Index (SPI) that is used to uniquely identify the Security Association (SA). It also contains a sequence number used to prevent an attacker from intercepting a data packet and playing it back at some later time and finally an authentication value generated by a message authentication algorithm. The principle can be seen in figure 1.7.

The most widely spread authentication algorithms are Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1). Both these algorithms make it difficult for an attacker to alter the authenticated data during transfer. This is achieved in the way that the sender calculates a digest or hash value from the data and includes the result in the authentication header. The receiver does the same calculation and then compares the results. If the data has not been altered in any way, the results will be identical. The hash algorithms have been constructed so that it is extremely difficult to change the data in any way and still get the correct hash. Since the proper authentication session key is also used by both calculations, an interceptor cannot simply alter the authenticated data and change the hash value to match. Without the session keys an attacker cannot produce a usable hash. MD5 produces a 128-bit hash and SHA-1 produces a 160-bit hash. Since the later algorithm was constructed by the National Security Agency of USA (NSA) some people do not trust it. The IPSec standard requires that the sequence numbers never cycle and that a new key is negotiated before the sequence number reaches the value of 2^{32}-1.

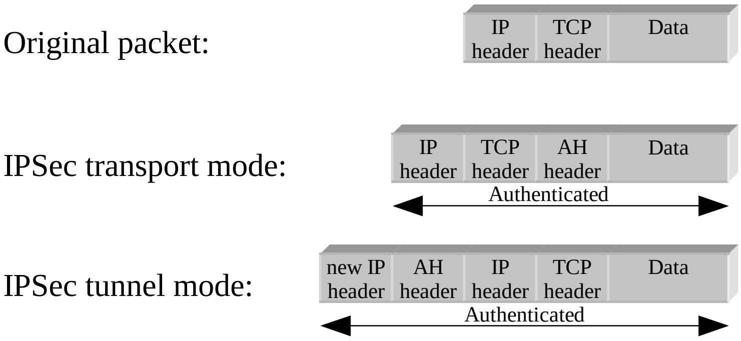


Figure 1.7. Principle of AH.

1.15.2.2 Encapsulating Security Payload

An ESP packet consists of three parts. *First* a control header containing a Security Parameter Index (SPI) that is used to uniquely identify the Security Association (SA). The control header also contains a sequence number field preventing an attacker from intercepting a data packet and replaying it at some later time.

The encapsulation can use one of several algorithms to encrypt the payload. The DES (Data Encryption Standard) algorithm is an example of a symmetric algorithm, which means that the same keying information is used both for encryption and decryption. These keys are exchanged via the IKE protocol.

The *second* part of an ESP packet is the original data payload, usually in an encrypted form to prevent anyone, except the receiver, from reading the original message. According to the IPSec standard it should be possible to turn off the encryption. However, if only authentication is wanted, the more powerful AH protocol described above should be used.

The *third*, and last part of the ESP packet is an authentication trailer. This part is optional but if it is used it contains an Integrity Check Value (ICV) that is used to check the authenticity of the packet. In the transport mode this authentication control offers some limitations compared to the AH case described below since it does not include the IP header in its calculations. In tunnel mode on the other hand its protection is total if both encryption and authentication are used as seen in figure 1.8.

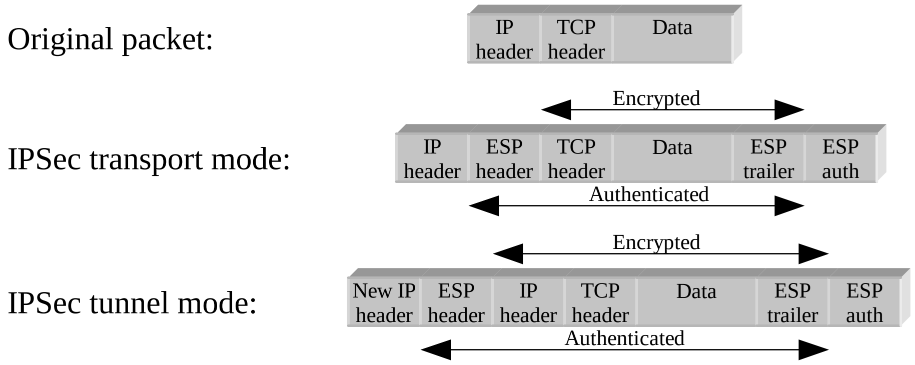


Figure 1.8. Principle of ESP.

1.15.2.3 Internet Key Exchange protocol

To encrypt and decrypt the packets the IPSec standard requires some kind of keys. The IPSec standard mandates that key management must support two forms of key establishment, manual and automatic.

The IKE protocol is a hybrid between ISAKMP (Internet Security Association and Key Management Protocol) [19], Oakley [20] and SKEME (Secure Key Exchange Mechanism) that are combined to provide a specific key management platform. Different portions of each of these protocols work in conjunction to securely provide keying information. (Note that different vendors often mix the words IKE and ISAKMP. ISAKMP addresses the procedures and not the technical operations as they relate to IPSec, while IKE best describes the IPSec implementation of key management.)

1.15.3 Key management

The IPSec standard describes several key management mechanisms.

Manual keying
The IPSec standard allows keys to be manually set. Manual key management requires that an administrator provide the keying material and necessary security association information for communications. Manual techniques are practical for small environments with a limited number of gateways and hosts. Manual key management does not scale to include many sites in a meshed or partially meshed environment. That is because every device must be configured and the keys must be shared with all corresponding systems. The use of manual keying reduces the flexibility and several features like re-keying and specific session keys are not possible to implement.

In practical implementations there are no obvious advantages of using manually keyed connections. However, they are useful when debugging the system, in case of errors, not having extra trouble with the automatic key exchange.

Automatic keying
When using automatic keying the correspondent hosts automatically negotiate the keys.

1.15.4 Establish a connection

IKE is complicated and several variations are available on the market. Simply put, IKE is based on the Diffie-Hellman key exchange protocol. The Diffie-Hellman algorithm is used to create a session key between two entities that have no pre-shared secret information. However, some kind of pre-shared secret is needed to authenticate both sides. Without such a secret the algorithm is not at all resistant to an active man-in-the-middle attacks, where the attacker impersonates each of the legitimate parties to the other.

The IKE connection establishment is divided in two *phases* (one and two). In each phase a different *mode* (main, quick, etc.) is used. These modes and phases are inherited from the Oakley and ISAKMP protocols, respectively. Below is a standard description that is used in many security implementations. This can vary slightly between different vendors.

Phase one
Phase one takes place when the two ISAKMP peers establish a secure, authenticated communication channel. This phase is initiated using ISAKMP defined cookies. The initiator cookie (I-cookie) and responder cookie (R-cookie) are used to establish an ISAKMP Security Association (ISA), which provides authenticated communications for the ISAKMP messages. A single ISA can and should usually be used for many second phase operations. In this phase the Main mode provides several messages to provide authentication services. The first two messages negotiate the policy and the second two messages exchange the Diffie-Hellman public data. Finally the last two messages authenticate the Diffie-Hellman exchange.

Phase two
Phase two is much simpler since it can use the keying material established in phase one to initiate a SA. The authentication was already done in phase one. This is the point where the key management is utilized to maintain the SAs for IPSec communications. Since ISAKMP is bi-directional either of the peers is able to initiate a Quick mode to establish an SA. The Quick mode is used to derive keying material and negotiate shared policy for the SAs.

After this, the SA is established and the transmission between the two hosts can be made in a secure way using ESP/AH. [21,22]

1.16 The need for standards

As in the rest of computering there is a strong need for standardisation. Products from different vendors must be able to communicate with each other, thus giving the customer the possibility to choose products from whichever vendor he desires without having to do a completely new investigation of the unique protocol that a vendor is offering. This also benefits the vendors because they do not have to develop their products from scratch. Instead they can focus on finding weaknesses and then develop improvements on the existing security protocols and algorithms such as IPSec and DES.

There are several organisations working in this area today for example ISO, ANSI, IEEE, and Internet Engineering Task Force (IETF). Often leading companies in the security area participate in these organisations.

An example of a national organisation that promotes standards in this area is the National Institute of Standards and Technology (NIST). It is an agency of the U.S. Department of Commerce's Technology Administration. NIST is trying to strengthen the U.S. economy and improve the quality of life by working with industry to develop and apply technology, measurements, and standards. This includes various kinds of cryptographic standards such as AES and DES (described in section 1.13.3 and section 1.13.5).

NIST works in tight cooperation with the National Security Agency (NSA) and therefore some people doubt their impartiality.

2 Security Related Companies

This chapter is a market research of existing security related companies, and briefly describes their business and products.

2.1 AcrossWireless

Across' product is the Wireless Application Delivery Platform (WADP). WADP is used in tandem with a wireless Internet WML browser on the mobile phone's SIM card.

All files (i.e., IMSI number, phone books, languages preferences, etc.) on the SIM cards can be updated and changed over the air (OTA) without the need for any additional physical equipment. This opens up a range of possibilities in managing subscribers SIM cards.

The product has support for multiple SIMs and OTA protocols, independent of SIM vendor. WADP also supports delivery of push services.

Because the applications are written in WML they are compatible with WAP and can therefore be used as WAP-applications.

AcrossWireless has been bought by Sonera, but are still developing their solutions.

Case study
The 5th of November 1999 Telenor Mobile, Norway's largest GSM operator, launched a mobile e-commerce service. The subscribers are able to order and pay for cinema and theatre tickets from their mobile phones, and when picking up the tickets they just have to show a control number to get the prepaid tickets. When ordering the tickets from the cellular phone, the user can choose whether he or she wants the money to be drawn from a bank account, credit card, or charged to the mobile phone bill. The technology behind all this is WADP and a SIM card with a WML browser.

2.2 Baltimore

Baltimore is a company that specializes in the development and marketing of a complete family of products and services to secure business conducted via computer networks, whether for Internet, extranet, or intranet applications.

The Baltimore product range includes a complete PKI system called UniCERT, cryptographic toolkits, security applications, and security hardware. [23]

2.3 Brokat

The company was founded in 1994 and is today established in 16 countries.

Brokat supplies software for e-business solutions, and is a big actor in the Internet banking segment. Its key product is the modular e-services platform "Twister" that provides the required technical infrastructure to fulfil the requirements of a modern e-

Business. Twister centers around an enterprise application server which forms the kernel of an e-commerce system. [24]

2.4 Celo

Celo Communications has offices in Germany, U.S.A., Ireland, Netherlands, and Sweden (Stockholm).

Offering a complete PKI solution, but nothing specific for the wireless market.

Their main product is CeloCom Enterprise. It consists of a complete PKI implementation (CeloCom Web, CeloCom PKI Manager, CA server, and CeloCom Enterprise Server) of which CeloCom Enterprise Server is the core product.

With CeloCom PKI Manager you can support your PKI structure, ranging from small local systems with a few users to full size on-line banking applications where hundreds of thousands of smart cards need to be issued. Together with the other products of the CeloCom family, CeloCom PKI Manager offers smart card support and strong encryption for intranet, as well as, Internet applications, i.e. e-mail and e-commerce applications.

CeloCom also offers smartcard technology and smartcard readers.

Supporting all platforms such as Windows 95/98/NT for clients and Windows NT, Sun Solaris, Linux, IBM UNIX, HP UNIX for the server software.

Supporting the standard cryptographical algorithms such as SSL, 3DES, MD5, SHA-1. [25]

2.5 Columbitech

A small Stockholm based company founded in April 2000.

Develops products for secure wireless data communication. Their main product is the Columbitech WAP Connector™. They call their product a corporate hosted WAP server and see Nokia as their main competitor. In the Columbitech WAP server the WTLS encryption of the WAP traffic is not decrypted until it has passed through the corporate control system. That means that the user will have to call an ISP that then connects to the requested WAP server. Note: This adds no security benefits in comparison with having your own WAP gateway. [26]

2.6 Entrust

Entrust corporation offers a wide range of security products ranging from simple programs that let you encrypt parts of your hard drive to full scale PKI solutions and advanced Virtual Private Network (VPN) solutions.

The Entrust.net division offers services concerning certificates. They issue both web server certificates and WAP server certificates. Entrust.net's CA is linked to one of the existing root CAs. The root CA linked to Entrust.net's CA is owned by Thawte Consulting. [27]

2.7 GemPlus

Founded in 1988. GemPlus is a global company with a branch office in Sweden.

A leading manufacturer of different kinds of smartcards, magstripe cards, microprocessor cards, memory cards, JAVA cards, etc.

Claims that smartcards are the ultimate portable security medium and therefore most suitable as the container for digital signatures. [28]

2.8 Melody Interactive

A Scandinavian-based company founded in 1998 with headquarter in Stockholm. Committed to delivering mobile Internet WAP applications and WAP gateways.

They state that for companies wanting their workforce to securely access the corporate network content even from outside the office, a WAP gateway with a security module supporting WTLS is the only secure solution. The Melody Wap Gateway works with Windows NT, 2000, Unix, and Linux.

Basically their solution can be categorized as yet another WAP Gateway, adding no new security in any way. [29]

2.9 MESC

The Mobile Electronic Signature Consortium (MESC) was formed in January 2000 and is an association of companies and organisations from the mobile phone and Internet sectors.

The main goal for the consortium is to establish and develop a secure cross-application infrastructure for the deployment of mobile digital signatures. The members are all working on the integration of mobile telecommunications and fixed connection Internet technologies to generate services that will require a mobile digital signature as a way to establish legal security for transactions performed.

Their current proposal for the mobile manufacturers is to add a new button to their mobile phones. The extension of the current pin-pad by a so-called sign button makes for a different quality from standard mobile phones. The sign button will exclusively be assigned a signature function.

Important members: GemPlus, Sonera, Brokat, HP, and Schlumberger.

Such a drastic proposal as a new button assumes that the leading phone manufacturers will adapt to the idea. Since none of Ericsson, Nokia or Motorola are members of MESC it seems a bit unlikely.[30]

2.10 OpenCard

Wants to develop a standard API for smartcards that makes it possible for users to use their smartcards in card readers from different vendors on different platforms. This would also enable the users to download any applications to their smartcards. [31]

2.11 PKI forum

The PKI forum, founded by Baltimore Technologies, Entrust Technologies, IBM, Microsoft, and RSA Security is an international, non-profit, multi-vendor alliance whose purpose is to accelerate the adaptation and use of PKI products and services.

The forum serves to bring customers and vendors together in a vendor-neutral setting to increase customer knowledge about the value of PKI and demonstrate how PKI solves the security issues for e-business. Through this effort the Forum envisages that it will accelerate the deployment of PKI and PKI-based solutions and show the high value of PKI as a trusted base for e-business applications.

Although a lot of security companies are members of the PKI forum none of the large mobile phone manufacturers are participating. [32]

2.12 Radicchio

Radicchio is an organization registered in the U.K. that was founded by Sonera, GemPlus, and EDS in September 1999. Its mission is to promote PKI in secure wireless e-commerce.

The main goals of Radicchio are:

- To achieve worldwide industry awareness of the opportunities presented by secure wireless e-commerce and PKI technologies.
- To become the industry voice and authority for PKI on personal wireless devices and networks.
- To enable a dynamic global market for secure wireless e-commerce through high-level standardization and technical collaboration and agreement between members.

The members of the organization spans over a wide area of companies such as certification authorities, mobile operators, systems integrators, device manufacturers, and software companies. A few examples of members are: AU-system, Baltimore, Ericsson, Gemplus, Sonera, and Schlumberger. [33]

2.13 RSA

As the name implies this company deals with advanced security matters. Investigating advanced security topics such as algorithms and other mathematical matters. They also offer several products such as a full scale PKI system called Keon.

They also offer a product called SecureID that is included in the R320 Ericsson mobile phone. It works similar to the standard ‘digipass’ used by most Swedish banks. That means that the user needs something he knows (password) and also something he has (the ‘digipass’ functionality) for access. [34]

2.14 Schlumberger

A major smartcard manufacturer with years of experience in the smartcard area. Schlumberger began it’s smartcard activity back in 1979 and in 1999 they announced that they had issued 1.5 billion cards worldwide. They offer a wide range of different kinds of smart cards and accessories. For example Schlumberger offers magnetic, memory and microprocessor cards for operators, developers, integrators and distributors worldwide. Furthermore, Schlumberger offers accessories; terminals for point of sale, ticketing, parking, and payphones; software and hardware tools for developers; servers and systems to manage networks and terminals, and to help companies harvest the benefits of smartcard solutions. [35]

2.15 SmartCard Forum

The mission of the Smart Card Forum is to accelerate the widespread acceptance of multiple application smartcard technology by bringing the industry leaders together in an open forum.

Important members: Baltimore, Celo, Cisco, Gemplus, Schlumberger, and RSA Security. [36]

2.16 TANTAU

TANTAU Software was formed in 1999. The company is headquartered in Austin, Texas, but it has development and sales offices in Finland, Germany, Switzerland, the U.K., and Australia.

The TANTAU WIP is a software product family that provides server-side at an enterprise, extending transaction applications to users with wireless devices.

The TANTAU Wireless Internet Platform supports a total wireless solution to connect various wireless devices to e-commerce applications and data sources. TANTAU's Wireless Internet Platform is distributed and can be configured with or without a gateway for conversion of mobile telephony to Internet protocols.

The server is compatible with Windows NT, Sun Solaris, and Tru64 UNIX.

Almost no specific information is available but it seems like they are selling an integrated server/gateway, i.e. once again the WAP gateway is placed at the company. [37]

2.17 VeriSign

This company offers a wide range of security products. The main product is their OnSite product that is a fully integrated PKI system that manages all kinds of computer networks; intranets, extranets, VPNs, etc.

VeriSign is also an issuer of digital certificates. VeriSign has issued over 215,000 web site digital certificates and over 3.9 million digital certificates for individual users. VeriSign issues both 128-bit SSL certificates and 40-bit SSL certificates. [38]

2.18 WAP Forum

This forum is the industry association that is responsible for developing the de-facto world standard for wireless telecommunication services on digital mobile phones and other wireless devices.

The major ambition of the organization is to bring all leading companies in the telecommunication industry together and thereby guarantee that the future telecommunication products will be fully interoperational and vendor independent.

Goals of the Wireless Application Protocol

- Will be proposed to the appropriate standards bodies.
- Independent of wireless network standard.
- Open to all.
- Applications scale across device types.
- Applications scale across transport options.
- Extensible over time to new networks and transports.

Almost all leading infrastructure providers, software developers and other organisations providing solutions to the wireless industry are members.[39]

2.19 WM-data

WM-data is a Swedish based company offering a product called E-mobilizer. It enhances security when accessing an Internet marketplace or a company intranet. The user needs to have an account registered in the E-mobilizer to be able to authenticate himself. WM-data cooperates with RSA and together they claim that they achieve true end-to-end security when combining their E-mobilizer and RSA’s SecureID. [40]

3 Electronic Currency

This chapter describes what electronic currencies really is and also looks a little deeper into some existing ones.

3.1 Introduction

Transferring money worldwide is nothing special today. People are getting used to paying their bills electronically and shopping with their credit cards. As the electronic infrastructure evolves we actually see and use less and less physical money.

Side by side to these changes an even more revolutionary situation is developing. The Internet has enabled a small financial revolution. Traditional currency systems can be replaced or will coexist with new Internet based electronic cash system. These cash systems are an alternative to the traditional financial systems where payments and transactions are always made in some existing currency (bound to a country and exist in a paper or metal form).

The issuers of electronic currencies could be seen as banks since customers can buy things for their electronic currency. A purchase of electronic cash with regular cash is much like a deposit in a bank. Nevertheless as long as the issuer of cyber currencies does not provide their customers with the ability to borrow money the common opinion is that they should not be seen as banks. In the future when Internet has grown even more powerful, these conditions might change and we will see several new virtual banks on the Internet all doing business in their own virtual currency.

Charles Cohen, the founder of Beenz.com, has raised an even more visionary prospect. He professes that in the future even private companies will start issuing their own currencies. He thinks that would be the real takeoff for electronic currencies because companies would be less dependant on the existing banks. The next step would be that companies could transfer currencies directly between each other making the banks and the standard currencies useless. [41]

The legal aspects of electronic money have been investigated in Sweden as early as 1997. The commission’s mission was to investigate what problems that may rise when mixing regular currencies with electronic ones and analyse if there was a need for any change in existing laws and regulations. The commission presented a framework for future electronic money legislation, but it was not really detailed since the European Union (EU) should develop a united policy for all its participants in this matter. Nevertheless the committee suggested some basic requirements that would assure financial stability and security. The committee also stated that all financial institutions should be able to issue their own electronic currency as long as they followed the stated guidelines. [42]

3.2 Two kind of currencies

There can be said to exist two types of electronic currencies; loyalty points and electronic cash. These two phenomena are distinguished and described below.

However, what is the purpose of these virtual currencies? Isn’t ordinary money sufficient any more? The electronic currencies add a new dimension to Internet sites. Electronic currencies are not quite like money. You cannot borrow it and you cannot inherit it for example. Instead electronic currencies represent a kind of value added service that makes it possible to tie consumers more tightly to their sites.

3.2.1 Loyalty points

An Internet site could for example give their visitors points for performing different assignments. These assignments could for example be telling a friend about the site or visiting a sponsor’s site. By rewarding the visitor with points the site makes sure, or at least more probable, that the visitor will return.

The loyalty points system also makes it easier to increase revenues from advertising since when visitors gets something for visiting for example a banner it is more likely that they really click the banner.

Another positive aspect with points is that a point can be worth a really small amount of money and still be attractive to the user since the points can be used to buy really low valued services. No one would click a banner just to earn 25 öre, but if the click instead enabled him to receive some kind of small value added service, like receiving a horoscope directly to his mobile phone the next morning, then maybe the point is worth clicking for. Since it is such a small effort for the customer to earn points, and thereby getting small value added services, they will come back to the site again.

3.2.2 Electronic cash

A more ‘money-like’ form of electronic currencies is the kind that actually can be bought with and redeemed for standard money. The electronic money can then be used in all Internet stores that accept that specific payment method.

The main difference from the loyalty points system is that the electronic cash typically can be used in a lot of different “stores” that sells a huge variety of different products. The loyalty points systems often are only used at a single site. Nevertheless in the future there might be an opportunity to actually exchange different kinds of points and electronic cash.

3.3 Existing types of currencies

There are a number of different types of currencies existing on the Internet today. Below a selected number of the most interesting and popular of them are described.

3.3.1 Beenz

Beenz is a typical loyalty program. The user opens a beenz account online for free and is then able to start earning beenz (i.e. loyalty points) by performing a number of different actions like for example shopping at or visiting certain sites. The earned beenz are saved in an account managed by the company until they are used to purchase goods or services from registered online merchants that are accepting beenz. [43]

3.3.2 CyberCoin

CyberCoin services are distributed through banks. The bank offers online merchants the CyberCoin service and offers consumers ‘wallets’. The merchants pay the bank for every transaction made and the amount is based on the transaction size. The bank then pays CyberCash a transaction fee for providing the technology and processing service.

The inventor of CyberCoin is CyberCash. They created the CyberCoin service to allow a consumer to use an existing bank account to transfer money to their ‘wallet’. Banks supporting CyberCoin provide the accounts that hold the money transferred to the ‘wallet’; enabling the money transferred to remain within the secure banking network. [44]

3.3.3 eCash

The eCash system is a single use token system. The user generates blinded electronic bank notes and sends them to his personal bank to be signed with his bank's private key. Then the bank signs the notes and withdraw the amount from the user's account. The signed notes are sent back to the user and are stored in the user’s software ‘wallet’ installed on the user’s PC.

eCash software uses digital signature technology based on public key cryptography to provide a high level of security. The algorithms used are RSA and 3-DES for the public key cryptography and SHA-1 when computing the hash function that is used to sign the transferred data.

To start using eCash for payments the user needs to open an eCash account and deposit money in it at any financial institution supporting eCash. That financial institution provides the user with the necessary eCash software. Thereafter the user simply chooses the eCash method to pay when visiting an eCash-enabled site. The eCash system supports micro payments as well. [45]

3.3.4 Flooz

Flooz is accepting credit card payment for gift certificates issued in an electronic currency called Flooz. The term Flooz is slang for cash in Persia. How a Flooz transaction works is described below.

On the Web site, users buy any amount of Flooz using a credit card. One Flooz equals one US dollar. A certificate and an electronic greeting card are mailed to the recipient, who can spend the Flooz at an affiliated online merchant, perhaps Cigar.com, swissarmydepot.com, or Toysrus.com. Flooz can be spent right away or stored in an account. [46]

3.3.5 Ipoints

An Internet reward program that enables e-commerce companies to reward their customers with loyalty points. Ipoints are earned when Ipoint members shop or interact with participating companies.

The user has to create an online account at Ipoint’s site. Thereafter the user can purchase a wide variety of things after earning the proper amount of Ipoints. [47]

3.3.6 Millicent

MilliCent is in live use only in Japan, but they are planning to introduce their services in both North America and Europe.

Millicent is a centralized token-based system. That means that the funds are held in the server hosted by MilliCent and not in the user's own PC. To be able to perform a purchase the user must open a MilliCent account: either directly with MilliCent or any MilliCent broker. The account can be 'filled' in three ways; online credit card transaction, billing their monthly ISP or telephone bill, or through pre-paid cards purchased anonymously through convenience stores. They support true micro payments with prices of less than a US. cent. [48]

3.3.7 Mypoints

A typical Internet reward program. Their program enables e-commerce companies to reward their customers. Mypoints are currently only availably in U.S.A., Canada, Australia, and South Africa. [49]

3.3.8 YadaCash

A loyalty points system run by the Swedish based company Goyada. By becoming a member and telling other users about the portal you can earn points that can be used to subscribe to different information services that are sent to your mobile phone. [50]

4 Mobile commerce

This chapter gives a background to the discussion about the future forecast of the mobile Internet. It deals with the mobile and Internet growth, services and common business development.

4.1 Introduction

First a definition of mobile commerce (m-commerce) should be established. The natural way to look at m-commerce is to consider it to be a subset of all e-commerce transactions. Therefore it can include several technologies as long as not all the actors are fixed in their locations. An important issue to consider is that to define a business as m-commerce it should involve some kind of economic transaction, it should involve more than just transferring data from one place to another. Although it is worth noting that the entire transaction need not take place on an electronic medium, even if much of it probably will, it could involve physical delivery of goods, for example flowers. The resulting business could still be categorized as m-commerce.

The appearance of mobile commerce provides a significant increase of value in the telecommunications sector. The two worlds of radio communication and data communication are emerging. This means that the Internet is extending into the mobile sector. This fact is also strengthened by the obvious fact that several standards, like WAP (section 6.1) and SAT (section 6.4.3) are being developed today. Some say these are necessary to further development towards a full-scale operating mobile Internet.

The mobile phone today must be considered to have be one of the most useful and popular technological devices in the last decade. As mobile technology evolves it is most likely that the border between different handheld devices such as PDAs, mobile phones, communicators, and even MP3 players, radio receivers, and GPS devices will disappear. It most probably will be the mobile phone that brings all these devices together. Nevertheless this will be several years in the future. Applications like videoconferencing using your mobile phone still are numerous years away.

Several reports agree that the mobile business will grow extremely large in the next couple of years. This is based on the prediction that by 2004, there will be around one billion users of mobile telephony. Furthermore there will be almost one billion Internet users. By this time it is also estimated that there will be about 600 million mobile Internet subscribers worldwide. Another interesting fact is that today less than 5 percent of all data are transmitted over mobile devices. This is expected to increase to about 25 percent in 2005. Predictions are that in two years m-commerce will represent 10 percent of all e-commerce. [51]

As seen below in figure 1.9 [52], Ericsson predicts that m-commerce will grow substantially after 2001 while the e-commerce on the regular Internet will continue to have only a linear increase.

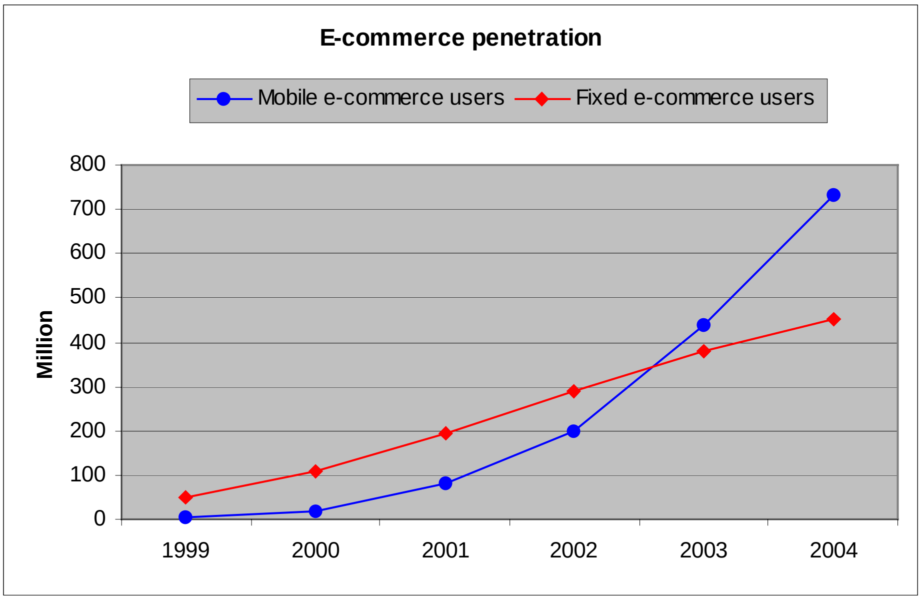


Figure 4.1. Predicted reach for fixed and mobile e-commerce.

4.2 Today's market

The mobile phone possesses a number of advantages that should be beneficial. You can always carry it with you. You can almost always be reached. Security matters are still a major problem, but solutions are emerging including a number of different techniques such as certificates, smartcards, and different kinds of cryptography. Already today different services based on location awareness are being developed. This will make the mobile phone even more attractive to the ordinary consumer. Another issue that is important in the m-commerce world is instant connectivity, this is a service that GPRS should provide. Therefore the user will feel like he is always online. This is a similar revolution to that we have witnessed during the last year in Sweden with the introduction of broadband.

4.3 Market drivers for m-commerce

4.3.1 Applications

The price for making a mobile phone call is falling due to the competition between different mobile operators. To prevent this from impacting their profits the operators must introduce value adding services to their customers. The question really is what kind of services the customers are willing to pay for. Being able to provide their customers with such applications would hopefully keep their profits from falling. Therefore there clearly is an incentive for different m-commerce applications, not only from the end user's perspective but also from the major mobile operators. Other actors that also are interested in such an evolution are of course the major mobile phone manufacturers since they are salosidized by the major operators.

The value of good applications can be motivated by looking at the explosion in use of SMS among the young Scandinavian population. Today this rather simple service is generating great revenue for the mobile operators. Evolving this service to additional value added services is what the future is all about. The future consumer is not interested in simply higher capacity or specific technical details, the consumer is interested in the applications he or she can make use of. That is what impresses new customers and keep them coming back, whether you are a mobile operator or a content provider on the Internet that wants to expand your business into the mobile market.

4.3.2 Mass market

Mobile communication has become a huge market all over the world. Therefore mobile penetration has also become a key factor when introducing new applications. Already today Scandinavia has a mobile phone penetration above 50 percent and that percentage will with no doubt continue to rise, especially when new services are available.

4.3.3 New technologies to make m-commerce become a reality

As mentioned before, the end user does not care about technology details. The consumer just wants to be able to use applications. Nevertheless the transmission rate is an extremely important factor when developing new services. Today the largest wide area radio communication standard in use is GSM. It only offers a transmission rate of 9.6kbit/s. Therefore the improvement of the radio communication network is awaited. These improvements often promise more than they can deliver. For example GPRS (section 6.2) was hyped to offer transmission speed up to 170kbit/s, but as the release date approaches the real transmission speed seems to drop substantially. The same procedure will almost certainly arise when introducing techniques like EDGE [53] and UMTS [54].

Nevertheless all the techniques mentioned above are together a key factor for achieving a true mobile commerce infrastructure, enabling the development of applications that the customers will are ask for.

4.4 M-commerce enabling applications

4.4.1 E-mail

The most obvious application a mobile user would benefit from is e-mail. Today this is an application that is used by almost everyone, everyday, everywhere. It has replaced most of the earlier use of fax. Therefore it is very likely that mobile customers would enjoy such an application.

4.4.2 Instant messaging and mobile chat

As popular as the Internet based ICQ program has become a mobile variant would most certainly be a great success. Such applications rely on the fact that the user is always connected to the net. Therefore GPRS is a necessary condition for such a service. An ICQ service combined with a location service would be even more interesting. This sort of service would replace the existing SMS service.

A similar service to instant messaging is chatting. This is a really popular service among young people surfing the Internet. Some applications using SMS technique are already available today, but as long as the SMS prices are as high as they are (at least in Sweden) these services will not become as popular as they could.

4.4.3 Mobile personal information management

Classical calendars have in the last couple of years been replaced more and more by small electronic PDAs. Enabling a similar application accessible from different kinds of devices, such as a mobile phone, would probably be an interesting alternative to most businessmen that today carry both their phone and their PDA. By enabling group calendars the different members of the project group could find out when certain members can meet.

4.5 Value adding services for m-commerce customers

This section focuses on the areas that are predicted to be most popular with a wide variety of users.

4.5.1 Banking

The online banking business has grown extremely quickly the last couple of years and today practically all banks in Europe offer their customers the possibility to perform different kinds of transactions over the Internet. This certainly is because of the fact that these Internet transactions save the banks a lot of money, so they can cut back on the expensive cost for managing their classic offices. Therefore mobile commerce is an alternative channel to let their customers initiate these cost saving transactions. Already there exist mobile banking solutions that include techniques such as the SIM Application Toolkit (section 6.4.3).

4.5.2 Vending machines

Paying for small purchases on your mobile phone bill is really interesting. This could typically mean that you pay for the newspaper with your mobile phone by dialling the phone number of the newspaper box. Sonera has implemented such a solution where the customer purchases a soda by dialling a number printed on the vending machine (see section 5.5.4).

An alternative to actually calling the vending machine would be to communicate directly with it using some other kind of technology, such as IR or Bluetooth.

4.5.3 Postal services

A lot of ordinary mail services could and probably will move from the traditional paper medium to the electronic one. All standard information like bills, payslips, and monthly bank account information could be distributed digitally direct to the receiver, saving the companies a lot of money.

4.5.4 Shopping and reservation

If you buy something you have to pay for it in some way. Therefore the mobile phone offers a great opportunity to both identify and to locate the customer. Once again, the communication can be both long-range (GPRS) and short-range (Bluetooth). The possibilities are practically unlimited. The consumer could for example order a pizza from the closest pizza restaurant. Another popular service would probably be reserving tickets using the mobile phone. The ultimate solution should then include some kind of confirmation between the mobile phone and a device situated at the check-in counter to completely eliminate the ticket.

Another area interesting to reposition to the mobile market is reservation of motels and restaurants. Once again this is a service that would benefit from location awareness.

4.5.5 Personal cards

The ability to update the telephone with personal information, membership cards, and transit cards would mean that the consumer would not have to carry around a lot of different magnetic stripe cards as they do today.

4.5.6 Information

Mobile information today primarily utilizes the SMS service. It can be either pushed or pulled to/from the consumer. Different systems use different techniques. In some systems the customer has to use an ordinary web browser to subscribe to the material he wants to receive. In other systems the customer sends a SMS with a ‘magic’ word specifying which service he or she wants to receive. A list of what could be interesting for consumers is listed below:

- TV and radio program/schedules.
- Conversions (temperatures, weight, length, speed, etc.).
- BMI calculations.
- Time schedules (buses, trains, flight etc).
- Guidance.
- Sport results.
- Stock information.

4.5.7 Entertainment

Computer games are a huge industry, especially after it became possible to play against other players over the Internet. This fact guarantees that gaming possibilities using your mobile phone would be really popular among consumers. That conclusion is backed up by the fact that even really simple games have become enormously popular. An example of this is the game called Snake on some Nokia telephones. There are several companies that are working in this area. One of them is Picofun that is focussing on developing WAP games for the mobile user.

Ever since Sony introduced their first Walkman, the possibility to listen to music on the move has been very popular. The existing MP3 technique could be integrated with the mobile phones. Already today you can listen to the radio using a small add-on that fits together with your Ericsson telephone.

Another popular form of entertainment is gambling and betting. This area will also most likely emerge as a mobile area. This would mean that betting companies could provide gamblers with more direct betting alternatives as the odds can be set in real-time.

4.6 Market sizing and forecasts

M-commerce is in a way a completely new channel that can be a complement to the more traditional sales channels represented, for example, by traditional e-commerce on the Internet. The content and service providers will be able to offer their customers a new way to initiate transaction. Observe that the number of potential consumers is growing.

The market for mobile phones has exploded during the last decade and it is continuing to grow very fast due to the availability of new and improved hardware (i.e. telephones) and more and more value added services. As seen in the figure 4.2 [55] the number of subscribers has and is predicted to continue to grow in the next couple of years. This forecast means that the number of subscribers will have risen from 90 million at the end of 1998 to approximately 240 million in the year 2003. Although these numbers refer to the European market, the rest of the world is predicted to follow similar trends.

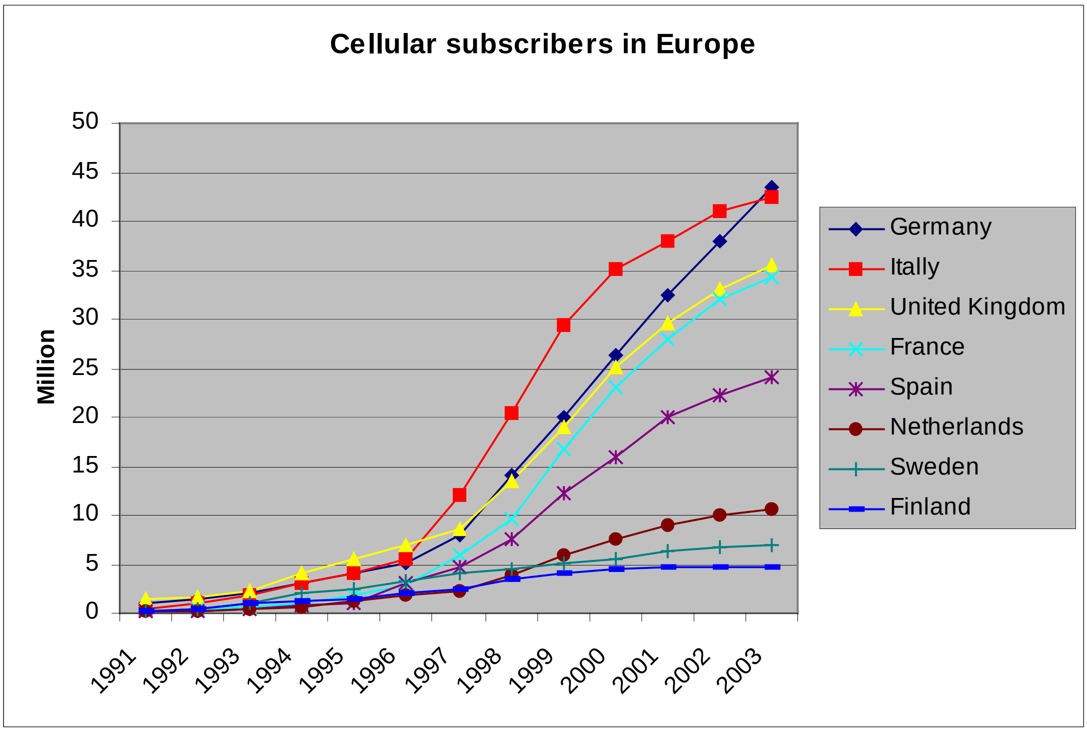


Figure 4.2. Predicted growth of subscribers in Europe.

In Europe alone the market for mobile commerce is estimated to €2.3 billion by 2003 [56], and by the same time the global market will reach $3.2 [57]. It will really take off with the introduction of new radio networks like GPRS and later EDGE and UMTS. Until GPRS is introduced SMS will be the main communication technique for applications. As shown in figure 4.3 [58] GPRS is predicted to finally penetrate the market in the year of 2003.

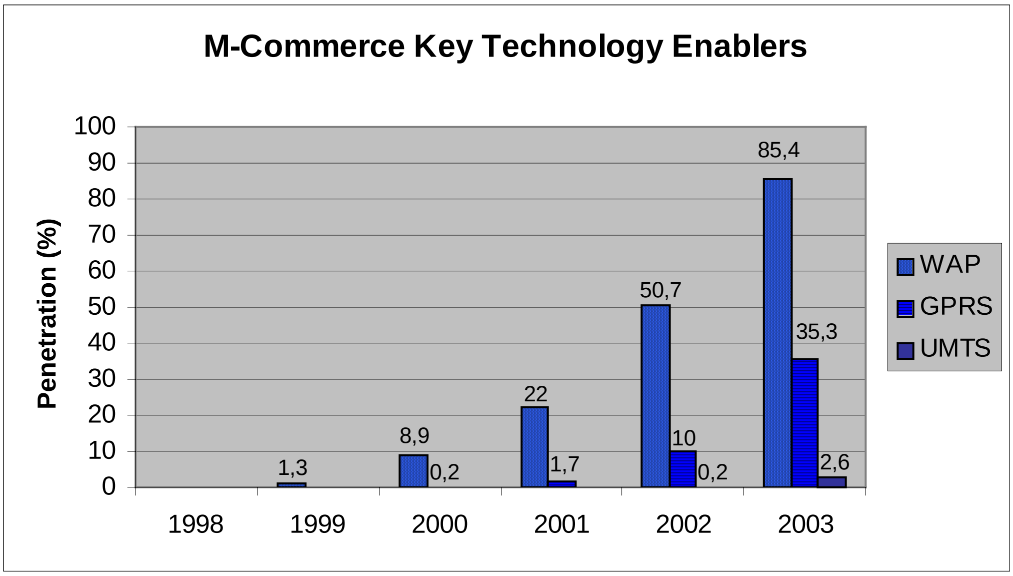


Figure 4.3. Predicted growth of m-commerce enabling technologies.

Another illustration of the growth of the mobile market is that there in the fall of 1999 there were about 300 million wireless users and about 200 million Internet users worldwide. Now predictions indicate that about 1 billion users will have both wireless and Internet access in the year 2003. [59].

The situation in Sweden has been investigated by a Swedish organization called ‘Radio Undersökningar AB’ (RUAB), which is doing market research in the area of modern communication. In their report [60] they compare the use of Internet in May 1998 with May 2000. Their investigation shows that during these two years e-mail has been the fastest growing application. This supports the results in other reports that show that e-mail would be one of the most appreciated value added services. The report from RUAB also shows that e-commerce still has not taken off. During the last two years there has been a modest increase from 3% to 3.5% of all Internet users. Due to an increase of Internet use during this time although the percentage difference is rather low it actually corresponds to an increase from 30,000 to 70,000 persons. Worth noting is that male Internet users are responsible for two thirds of all purchases done on the Internet. The result from their investigation is shown in figure 4.4 [61] and figure 4.5 [62].

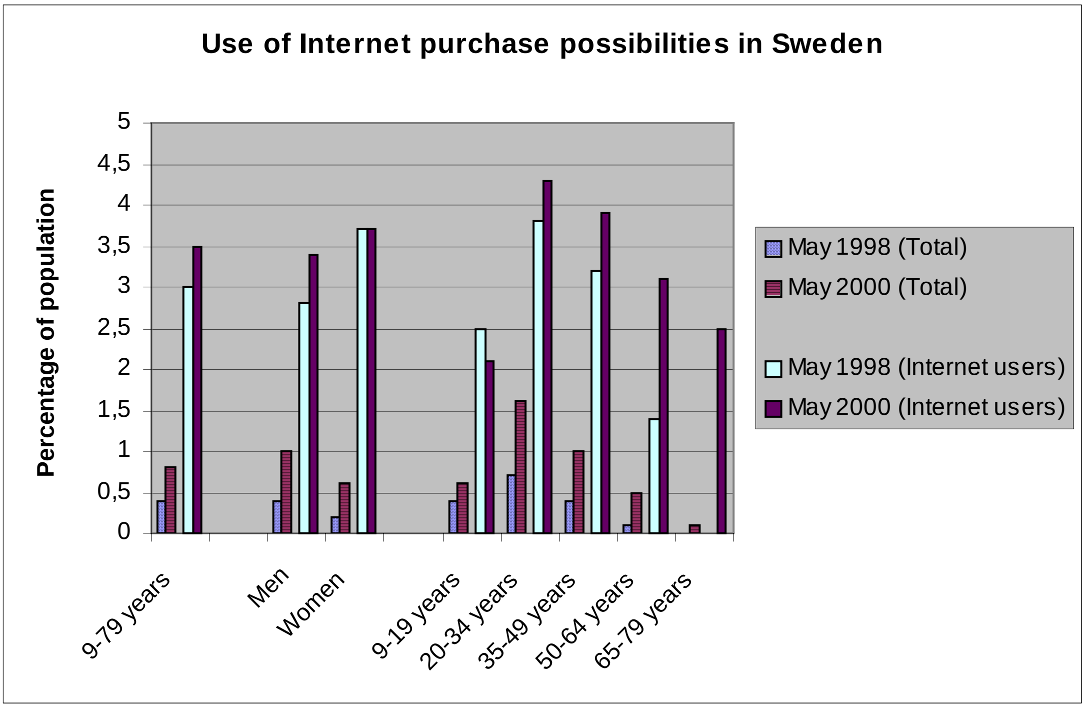


Figure 4.4. Purchases made using the Internet.

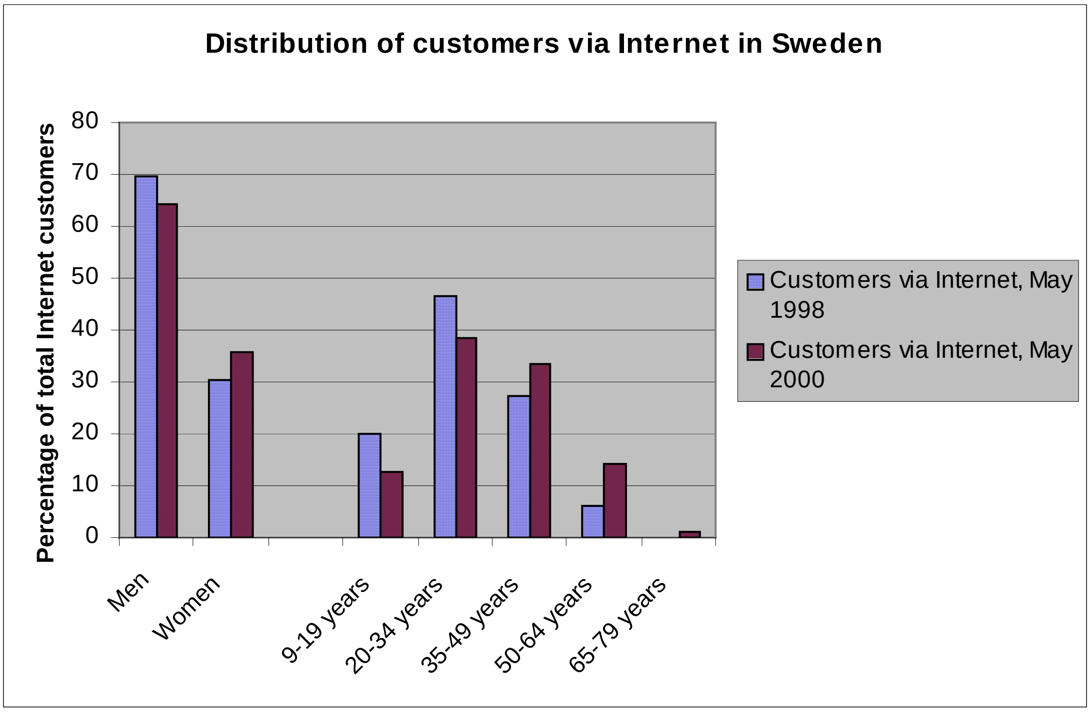


Figure 4.5. Distribution of Internet customers.

Although it is hard to know how these statistics relate to the mobile market the positive trend for e-commerce will most likely reflect positively on m-commerce. [63]

There exist a common opinion that we will se an enormous increase in the m-commerce market. This is substantiated by the Durlacher report. This is shown in figures 4.6 and 4.7 below [64].

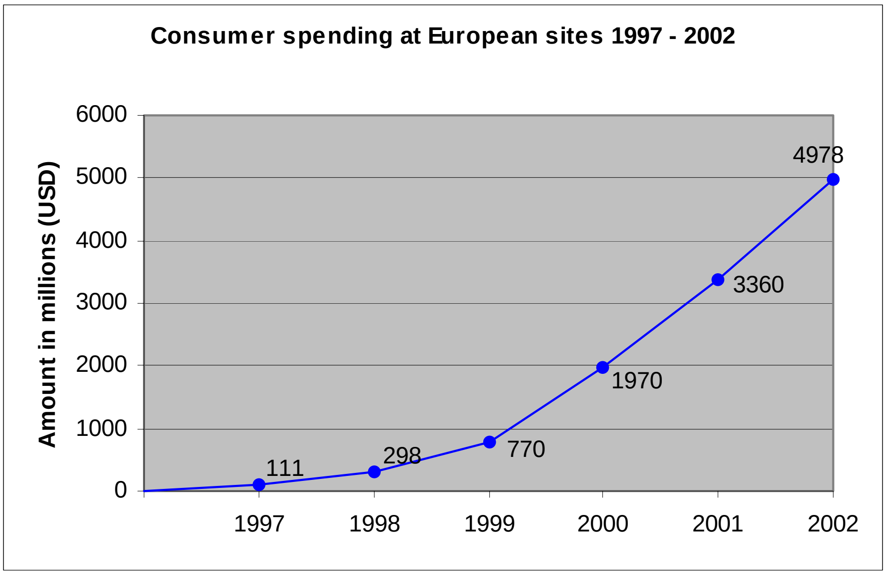


Figure 4.6. Expected growth in e-commerce.

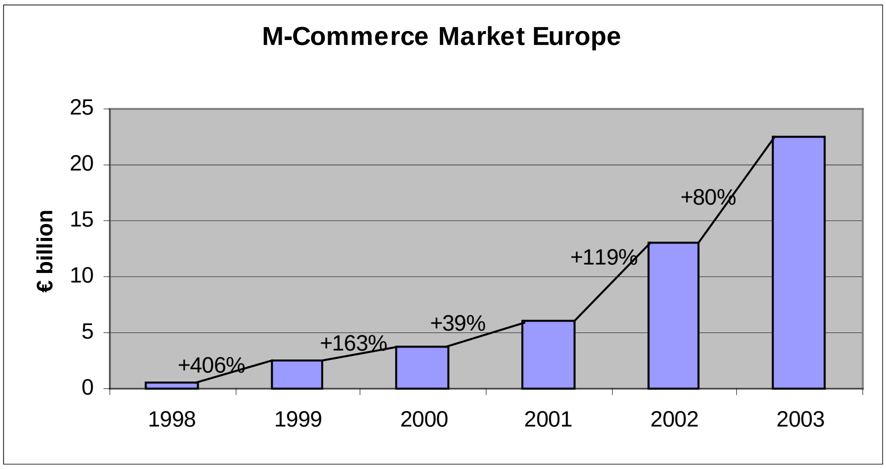


Figure 4.7. Expected growth in m-commerce.

As the mobile Internet spreads many content providers want to get paid for the information they are providing. This, surprisingly, rises some problems. Consumers used to the Internet expect these Internet like services to be free. Therefore the content providers that offer mobile services most likely will have to find their income through a variety of channels. The first is to think about commercials. Although it is a way that probably will not work as good as on the Internet since the distribution media offers such limited display opportunities. Another way to make money is revenue sharing with the mobile operator.

Nevertheless, the Durlacher report predicts that advertising will become the main income for m-commerce companies. They estimate that the annual revenue will be €5.4 billion once m-commerce has become an accepted way of trading. As the second highest revenue source the Durlacher report predicts financial services since it is a type of service that attract people from all age groups. The rest of the predictions are shown in figure 4.8 [65]. Notable is that mobile shopping is predicted to be the third largest source of revenue.

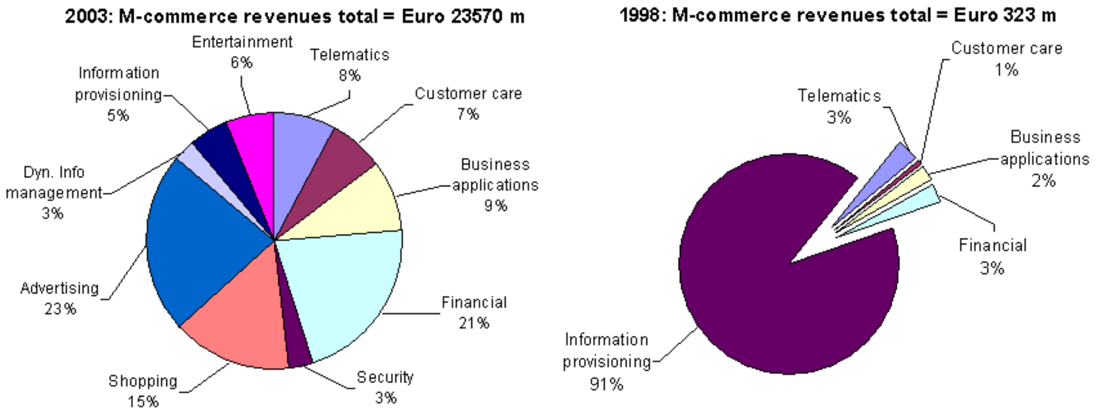


Figure 4.8.Expected change of revenue in m-commerce.

4.7 Mobile portals

Mobile portals are very similar to the ordinary portals on the Internet. What differs is the limited possibilities for interaction with the user. The information must be really personalized and never more than a few clicks away. A study of the user behaviour towards different interfaces shows that consumers are 50 percent less likely to access a feature on their phones if it requires pressing a button [66]. Therefore few will search for information on a mobile portal. Therefore the information has to be extremely personalized.

You may wonder if there really is a big market for companies offering mobile value adding services. Of course there is a demand from costumers to be able to use their mobile phones for more than just calling. Nokia released a report [67] on the demand for mobile value added services in early 1999. Although the telecommunications area is an rapidly changing market the result of that market research can still be valuable since Finland has a lead position in this area. The Nokia investigation showed that a majority, 86.8%, of the consumers stated that they were at least a little bit interested in mobile value added services. The top requests from the Nokia reference group is shown in figure 4.9 [68]. These are the most demanded services from the positive people that showed the most interest in value added services, but those who were less positive had almost the same ranking.

Value added service	**Level of interest (%)**
Bank	86.4
Phonebook	81.5
E-mail	80.0
City navigation	73.8
Remote control	72.7
Ringing tones	72.3
Dictionary	71.2
Weather	67.7
Pizza order	59.1
News items	55.4
Travelling businessman	52.3
Big event	37.9

Gambling	33.8
Sports	33.3
Stock info	32.3
Grocery store	31.8
Stock portfolio	30.8
Leisure time	27.3
Jokes	24.2
Sunrise	19.7
Daily biorhythm	10.6

Figure 4.9. Requested value added services.

Some of these features, like phonebook and ringing tones, have already been available for a very long time still they are considered to be highly ranked by the consumers. Worth noting is also that merely entertainment is not seen as that appealing. [69]

5 Payment methods

This chapter describes different kinds of payment methods and solutions. The solutions mentioned are mainly focusing on the Swedish market.

One of the most important things in the business area has always been to be able to pay for whatever goods you are dealing in. In this aspect the electronic online environment is no different from the usual offline world. The most common way to shop online is using some kind of credit card. Another possibility that has become reality in Scandinavia is to use one's Internet bank office to pay for merchandise purchased on the Internet. This service is in Sweden called direct Internet payment and is offered by all major domestic banks.

Celltribe is in some way in a unique situation. Since we aim to deliver electronic merchandise over the Internet, some of the regular aspects of commerce become a bit of a problem.

Complaints necessitating a refund could become a problem since the possibilities to prove that the purchased goods have been delivered is not that easy.

5.1 Internet payment systems

The Internet payment systems currently in use or under trial fit into two categories: account-based or token-based.

5.1.1 Account based

Account-based payment systems link each user – whether a consumer or a content provider – to a specific account. The most common type of account-based system is the credit card payment system, where the consumer submits his or her credit card number and expiration date in some kind of secure form, most likely via SSL. The information is retrieved by the merchant, who then can debit the consumer's account. This payment method does not provide security against fraudulent use of credit card details. Note that the SET standard has been developed to facilitate secure transactions using credit cards and could be seen. A more secure account-based payment system is direct payment through an Internet bank, where the user logs into the bank in his or her usual way, with all the security typically provided by the user's bank, and there confirms the payment.

5.1.2 Token based

When talking about token-based payment systems, we mean either some kind of electronic cash, like the global external beenz solution, some kind of internal loyalty-point system like Celltribe's CellPoint system, etc. These kinds of systems can handle micropayments down to fractions of a cent, although the user in some way is required to exchange his or her 'real' money into the specific cyber-currency.

5.2 Performing transactions using credit cards

Financial transactions where the customer cannot physically see who he or she is trading with have always caused reluctance because the customer feels more insecure. This is of course also the situation on the Internet. Considering that the most global paying system is the credit card system of course shows that this problem can be addressed. The credit card system has been marketed and built up over a long period of time and is today accepted almost all over the world. Nevertheless, the credit card system of today causes some problems and limitations. Especially in Europe the use of credit cards online is hindered by national legislation, since some countries do not allow online credit card transactions because these are considered not as fulfilling the requirement that all card transactions must be physically signed by the cardholder.

As the e-commerce market is growing with an enormous speed the credit card companies want their customers to be able to use their credit cards all over the Internet, independent of their nationality. Therefore on February 1, 1996 the two largest card companies, Visa and MasterCard International, announced that they had the intention to develop a world standard that would solve this not-physically-present-problem. The standard was to be called Secure Electronic Transaction (SET) [70]. This initiative evolved and on December 19, 1997 a consortium called Secure Electronic Transaction LLC (SETCo) was formed to implement the SET specification. Today the SET standard is being promoted both by the credit card companies and the banks.

5.2.1 Techniques used in the SET standard.

The SET protocol uses a various kind of techniques to protect all three parties of the transaction: the consumer, the merchant, and the financial institution. Privacy is guaranteed using both asymmetric and symmetric cryptography. In the asymmetric variant RSA is used for signatures and to encrypt the session keys that vary between each transaction. The symmetric cryptography uses the DES algorithm to encrypt the data that is sent during the transaction.

Integrity is also provided by the SET protocol. This is simply done by using a hash algorithm in combination with the sender’s private key and thereby producing a unique digital signature.

The third important factor concerning security is authentication. The SET protocol solves this issue by using certificates. A trusted third party, called a Certification Authority (CA), supplies the certificates (See section 1.12.2). [71]

5.2.2 Payment transaction

SET is a transaction protocol. It is used when the consumer decides to buy something from a merchant situated on the Internet. The SET requirements must be fulfilled by all three parties regarding specific software and hardware to enable a SET transaction.

The first thing that happens is that the merchant separately sends two certificates to the consumer. His own certificate and the acquirer’s (The financial institution or its agent that acquires from the merchant the financial data relating to the transaction and initiates that data into an interchange system) certificate as well. The consumer’s software validates both these certificates and if none of them are on the revocation list, he sends his own certificate together with the encrypted payment data to the merchant.

At the merchant the payment data is decrypted, but all other information, card number, expiry date and charge authorization request, is sent on to the acquirer. Therefore the SET protocol protects the customer’s credit card information even from the merchant. Since the merchant does not see the actual credit card information.

When the acquirer receives the consumer’s credit card information and decrypts it. Thereafter the acquirer checks that the consumer has the right amount of money/credit for the transaction. This check is done with the consumer’s bank. The response from the bank is encrypted and sent back to the merchant. This message approves or denies the purchase to take place. The merchant sends the same message to the consumer. This, assuming that the transaction was approved, means that the purchase is confirmed.

Finally, the merchant tells the acquirer that the actual transaction is ready to be performed. The acquirer manages all the necessary communication with the consumer’s bank.

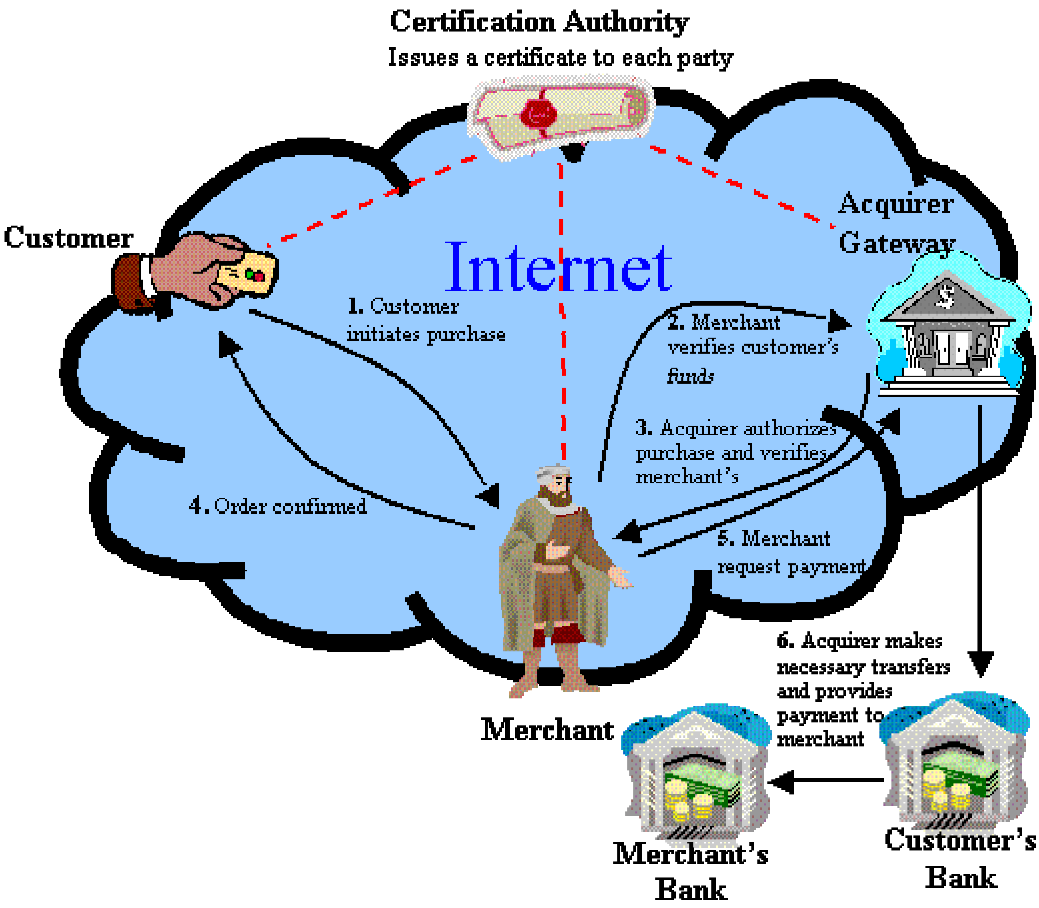

Certification Authority
Issues a certificate to each party
Customer
Internet
Acquirer Gateway
1. Customer initiates purchase
2. Merchant verifies customer’s funds
3. Acquirer authorizes purchase and verifies merchant’s
4. Order confirmed
5. Merchant request payment
6. Acquirer makes necessary transfers and provides payment to merchant
Merchant
Merchant’s Bank
Customer’s Bank

Figure 5.1. Description of SET transaction.

5.2.3 MIA

MIA stands for Merchant Initiated Authorisation [72]. This is a simplification of the SET standard that does not require the consumer to be SET connected. All information between the consumer and the merchant is sent using regular SSL protection. Between the merchant and the acquirer the SET standard is used as described in section 5.2.2.

5.2.4 Signature on file

This is a variant of MIA. The merchant gets a permanent authorization and provides the consumer with a unique password. The customer thereby accepts that the merchant is free to store his credit card information, but may use it only if the customer approves by providing the merchant with the password. In this variant the credit card information is transferred a maximum of one time over the Internet. Between the merchant and the acquirer the SET standard is used as described in section 5.2.2.

5.2.5 Enabling SET transactions

To be able to perform SET/MIA transactions one needs two things. First of all a card redemption agreement (in Swedish ‘kortinlösen avtal’) with a bank. The second thing that is needed is access to a SET engine, either your own or an engine run by a third party.

In 1989 the owners of Nordbanken, Handelsbanken, Föreningssparbanken, and Östgöta Enskilda Bank founded a company called CEKAB. The company’s business concept is to provide a secure and cost effective processing environment for electronic card based payment transactions. They also certify that different SET products are integratable in the Swedish environment. They recommend SET engines from three different vendors:

- GlobeSET [73].
- IBM Payment Manager [74].
- Trintech [75].

Their products are however rather expensive for example, the IBM product costs 132,000 SEK. Therefore is it not profitable for a small company to invest in such a product since they will not perform enough transactions to justify the cost.

An alternative for investing in your own SET engine is to use a so called SET hotel that is administrated by a third party. In this solution the merchant communicates not directly with the bank, but through the SET hotels’ SET engine. This solution has both positive and negative features.

Positive aspects:

- No extra direct hardware or software investments for the SET engine.
- No direct cost for maintenance, upgrading, and administration of the SET engine.

Negative aspects:

- Higher security demands on the communication between the merchant and the SET hotel.
- Less control. The merchant can only check the transaction via an API. The merchant cannot observe the transactions live.
- Contracts must be signed between the merchant and the SET hotel. The merchant will still need a card redemption agreement with a bank.

Once again CEKAB recommends several such companies [76]. There are also several foreign payments hotel that offers the opportunity to perform credit card transactions. Foreign hotels are not as positive to SET as their Nordic counterparts. Below are a few examples of both domestic and foreign payment hotels:

- NetGiro International AB
- DebiTech
- SecureTrading

5.2.6 The situation in Sweden

All domestic banks in Sweden require that the merchant use either SET and/or MIA. If the merchant is using the original SET standard then, the bank guarantees the transaction. If the merchant is using MIA on the other hand, and thus the consumer has not signed the transaction, therefore the bank does not guarantee anything. The complete risk of not getting paid lies on the merchant.

5.2.7 Prices

The credit card companies do not regulate the prices. Therefore there exists a competition between the different banks. There is also a distinction in prices between different types of cards, such as credit cards, debit cards, and bank cards. There can also be a difference between cards issued by a Swedish bank and cards issued by a foreign financial institution. Often there is also a distinction in prices between SET transactions and other, for the bank less secure, transactions.

	Nordbanken	**SEB**	**Föreningsspar Banken**	**Handels Banken**	**Telia Säker Handel**	**NetGiro**	**Debitech**
Initial cost	*	*	*	*	5000+2000/bank	18,000	25,000
Monthly cost					2000	750	500
Transaction cost	?	3-6 SEK + 2.3-2.6 %**	5 / 5+2.3%***	?	8	4	Max 4% (lowest 2,8%)

Figure 5.2. Credit card prices in SEK.

* Note, if a Swedish bank is chosen to be card redempter then the merchant has to purchase a SET engine or use a SET hotel.
** Initial cost for Swedish bank cards + percentage for foreign cards. The price varies with the volume.
*** Swedish cards / Foreign cards.

5.3 Direct payment through an Internet bank

The following sections describe each major bank and what services they can offer companies that want to utilize their services. All Direct Internet Payment require that the company must have an account in the specific bank since all transactions are made between internal bank accounts. The money could then be transferred to another bank on a regular basis.

5.3.1 SEB

Requirements on the company's web site

The bank has several demands on any company that wants to utilize its service. All communication involving exchange of personal information between the company and the customer must be protected by SSL. SEB also demands that all ordering of products take place via SSL protected pages. Another feature that the company must provide is a firewall that protects against trespassing.

The contract also clearly regulates the handling of the order reference number. That is because this number is the unique identification of a completed transaction. The current version of the SEB solution does not support handling of the problems with refunds. These matters must be taken cared of in the offline world.

The company should not rely on the automatic feedback that an order is carried out. Instead the company should use a feedback routine to check that the transaction has been successfully carried out. This means that it is the merchant that must take the initiative to actively check all transactions.

Payment procedure
A typical payment procedure is described in the figure below. All numbers describe some kind of communication and are described in a little more in detailed below in figure 5.3 [77].

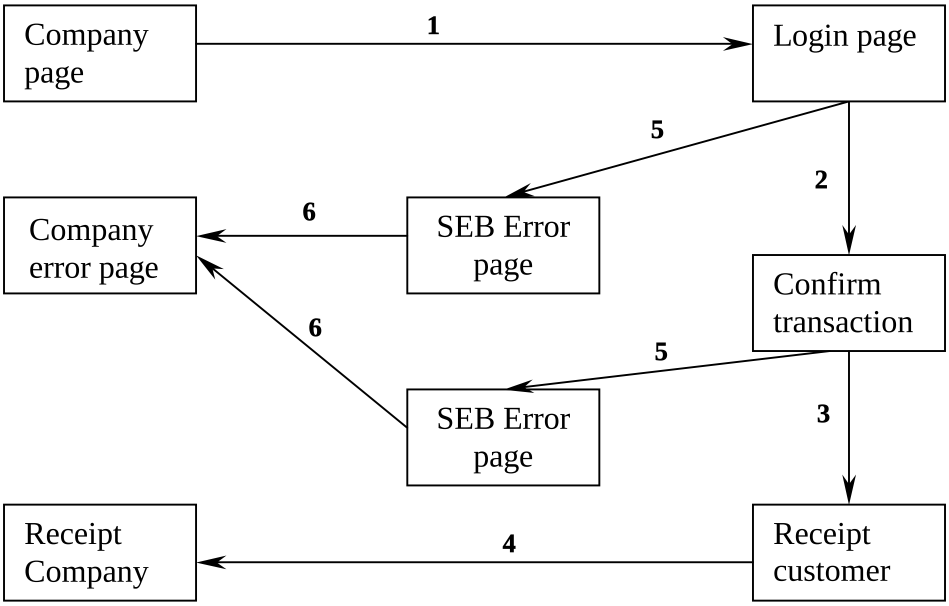


Figure 5.3. SEB's transaction system.

1. The company puts together all necessary parameters and posts them to the bank, where a logon page is presented for the customer that wants to perform a transaction.
2. The customer logs in using a ‘digipass’. If the login is successful the customer comes to a page where the order number and the amount of money for the purchase is presented. The customer simply chooses which account he wants to pay with. He confirms the transaction by generating a unique signature with the ‘digipass’.
3. As a receipt of the transaction the customer sees a receipt page. On that page he can choose to follow a link back to the merchant's site. The address and contents were sent by the company to the bank as one of the parameters described below. Note that the customer is not, by any means, obligated to follow this link back to the company. The customer has already performed the transaction.

4. If the customer chooses to follow the link back to the company, then the company can be sure that the transaction really has been completed.
5. If the login procedure fails an error page is presented with a return link to the company that the customer can choose to follow.
6. The customer can choose to follow the link to the company's own error page.

The receipt to the company is not generated automatically. Therefore a company selling electronic merchandise that should be delivered instantly (in contrast to mail order businesses) must actively watch when their customers perform their transactions. For a mail order one probably is willing to wait for days for the merchandise to arrive, but for electronic goods the waiting time is expected to be much shorter.

The transaction parameters

Below is a description of the parameters that are transferred from the company to SEB during a transaction. Note that if the data description is numerical characters zeros should be added so that the length of the parameter always is as described in the table below. If the data description is purely characters then spaces should be added instead of zeros to fill the field.

Note that all parameter description in the tables below is taken from SEB's manual [78].

Parameter	Data description	Additional information
SÄLJFÖRETAGID	8 numerical characters	This code is unique for every company using SEB's service Direct Internet Payment. SEB provides the number to the company.
ORDERNUMMER	10 numerical characters	Unique number that identifies the order. If less than ten characters, zeros should be added to the left.
ORDERBELOPP	9 numerical characters	The two characters to the right are always ören. The minimum transaction is 1 SEK and the maximum is 200,000 SEK.
BESTÄLLNINGSTID	14 characters (yyyymmddhhmmss)	Date and time when the company registered the order.
SISTA_BETALTID	14 characters (yyyymmddhhmmss)	Optional parameter (14 spaces). If included, the transaction must be performed before this time.
GICK_BRA_URL	80 characters	The URL that SEB should present to the customer if the transaction was successfully performed. *
GICK_INTE_BRA_URL	80 characters	The URL that SEB should present to the customer if the customer wants to discontinue the transaction or if anything goes wrong in the system. *

Figure 5.4. Parameters sent from the marketplace.

*Note: The customer must actively choose to use this link. It is not done automatically. Also note that if the URL is shorter than 80 characters it should contain spaces so that the total length of the transferred URL is 80 characters. If the URL contains an ampersand (&) then the corresponding hex code (%26) should be transferred instead.

All these parameters are concatenated forming a long string (no separators are used). The string is then input to a crypto module that is supplied by SEB. The crypto module returns an encrypted string called D2. This string should be put in a form and be of the type "hidden" when it is transferred to SEB.

As mention above the company might not be notified that the transaction has been performed. Therefore SEB provides the company with the possibility to actively watch its orders. The company constructs a string containing a number of order reference numbers (maximum 50), encrypts it with the same crypto module as above and sends it to the bank. The transmission is done using SSL and the encrypted string should be called D1. When SEB receives the string it is decrypted. Thereafter SEB checks the status of the submitted orders. This information is then returned to the company. The parameters involved are described below.

Parameter	**Data description**	**Additional information**
SÄLJFÖRETAGID	8 numerical characters	The unique company code provided by SEB.
TIMESTAMP	14 characters (yyyymmddhhmmss)	Date and time when the company registered the order.
SIGILL	32 characters	Elective text provided by the company. Is returned unchanged to the company from SEB.
ORDERNUMMER	10 characters	The orders that the company wants to check.

Figure 5.5. Parameters sent to control a transaction.

The response from SEB is always sent unencrypted (plain text). The company can choose to get the response parameters with or without the amount of money included (BETALBELOPP), as described in the list of returned parameters below.

Parameter	**Data description**	**Additional information**
TIMESTAMP	14 characters (yyyymmddhhmmss)	Date and time when the order was handled by SEB.
SIGILL	32 characters	The seal unchanged.
ORDERNUMMER	10 characters	The order reference number in return.
BETALNING_OK	1 character	Success return code. Y = transaction OK, N = transaction NOT OK
BETALBELOPP	9 numerical characters	The two characters to the right are always ören. The minimum transaction is 1 SEK and the maximum is 200,000 SEK.

Figure 5.6. Parameters returned to the marketplace.

Prices

Note that the price does not include any exposure on SEB's web pages. The price of such a service is negotiated in a separate contract.

• Initial cost:	2000 SEK.
• Monthly cost	200 SEK.
• Transaction cost	10 SEK or 5 SEK + 2%.

5.3.2 Handelsbanken

Requirements on the company's web site

Handelsbanken has several requirements on the company that wants to utilize their service Direct Internet Payment. All communication between the company and the bank must be protected by SSL. Another demand is that the company must provide a firewall that protects against trespassing. The contract also points out that this is not only a digital matter. Both parties must have administrative routines and tools to be able to detect attacks upon their separate parts of the system.

The company must also ensure it does not discriminate against the bank's customers in any way. This includes discriminating against other payment forms or other banks corresponding services. This discrimination could for example exist if Celltribe provided a bonus amount of CellPoints to the customers that are using another bank’s corresponding service.

Furthermore Handelsbanken declines all involvement in case of any complaints concerning the product that the customer might have regarding for example refunds.

Payment procedure

The company is linked to Handelsbanken’s server using a standard form. The form contains a number of fields that are all filled in by the company and is of the type ‘hidden’. Below is a description of the exact parameters that are transferred from the company to Handelsbanken during a transaction.

Note that all parameters with a data description including the word ‘max’ can have the stated number of characters, but could have less. No padding is necessary.

Note that all parameter description in the tables below is taken from Handelsbanken’s manual [79].

Parameter	Data description	Additional information
BUTIKID	String, 4 numerical characters	This code is unique for every company using HB’s service. HB provides the number to the company.
ORDERNUMMER	String, max 10 numerical characters	Unique number that identifies the order.
ORDERBELOPP	String, max 9 numerical characters	The amount of the transaction. The two last characters to the right are always ören. The minimum transaction is 10 SEK.
RETURURL	String, 150 characters	The URL that Handelsbanken shall link back to the customer, i.e. the page that confirms the transaction in the company’s system.
KONTROLLSUMMA	String, 32 characters	A checksum that is used to confirm that no changes have been made during the transfer. The checksum is produced using the different parameters plus a shared secret that HB and the company have agreed on. The algorithm used to produce the checksum is the well-known MD5 algorithm.

Figure 5.7. Parameters sent to the bank.

The customer performs the transaction, authenticating himself in his regular way at Handelsbanken using his preinstalled certificate. Thereafter he is linked back to the URL (RETURURL) that the company supplied in it’s initial form. Below is the description of the parameters that are included in the return form.

Parameter	Data description	Additional information
BUTIKID	String, 4 numerical characters	The unique company code provided by Handelsbanken.
ORDERNUMMER	String, max 10 numerical characters	Unique number that identifies the order.
ORDERBELOPP	String, max 9 numerical characters	The amount of the transaction. The two last characters to the right are always ören.
STATUS	String, 1 numerical character	Success return code. 0 = transaction OK, 1 = transaction NOT OK.
TIMESTAMP	String, 14 characters (yyyymmddhhmmss)	Date and time when the order was handled by HB.

KONTROLLSUMMA	String, 32 characters	A checksum produced by the above parameters and a shared secret that HB and the company have agreed on. May not be produced if something goes wrong in an early stage (Status = 1).

Figure 5.8. Parameter returned from the bank.

By checking both the status variable and the checksum the company can be sure that the transaction actually has been performed.

5.3.3 Föreningssparbanken

Requirements on the company's web site
Föreningssparbanken (FSpa) have several requirements on companies that want to use their service, Direct Internet Payment. The demands are of both technical and administrative nature.

All commerce should be protected by SSL. The marketplace should be run on a dedicated server. The server should for example not be supporting additional services such as mail server, news server, etc. FSpa also requires that the server that is running the marketplace is well secured, which includes a firewall, components not in use should be removed, non-necessary services should be turned off in the configuration, etc.

There should also exist administrative routines and tools to deal with security issues, such as detecting intruders. There should also exist administrative routines for analysing the logs. Furthermore the security solution must be well documented and the people from FSpa shall have the right to check in detail that all necessary security actions above have been taken care of.

Payment procedure
An important part of the Föreningssparbanken's system is the signing module. It is available in JAVA, C, Perl, or ASP environment. It is used to make sure that a transaction really is initiated from the company it is claimed to be. The signing module is also used to watch that the transactions really have been performed.

The input to the signing module is all parameters described below concatenated into a single string with fields separated by a '#'. The input to the signing module varies in the different implementations. In C for example the signature module needs a second argument, the signature string, which is the parameter the module uses to return its response to the calling module. This is not the case in JAVA.

After the signing module is finished all data is POSTed using SSL.

The necessary parameters that need to be transferred from the company to the bank are described in detail below. Note that all parameters with a data description including the word 'max' can have the stated number of characters but could also be fewer. No padding is necessary. Also note that all parameter names are in lower case.

Note that all parameter description in the tables below is taken from Föreningssparbanken's manual [80].

Parameter	Data description	Additional information
Ordered	max 10 numerical characters	Unique number that identifies the order. Is used to later identify that the transaction has been performed.
Butikid	max 16 numerical characters	This code is unique for every company using FSpa service. FSpa provides the number to the company.
Belopp	max 6 + 2 numerical characters separated by a ’,’	The amount of the transaction. The two last characters after the ‘,’ are ören. The maximum transaction is 10,000 SEK.
Timestamp	max 9 numerical characters	For future use. UNIX implementation accepts normal timestamp syntax, otherwise ‘0’ is the only acceptable value.
url_ok	max 120 characters	The URL that FSpa should present to the customer if the transaction was successfully performed.
url_nok	max 120 characters	The URL that FSpa should present to the customer if the customer wants to discontinue the transaction or if anything goes wrong in the system.
Sig	48 characters	A checksum that is used to confirm that no changes have been made during the transfer. The checksum is produced using the different parameters above.

Figure 5.9. Parameters sent to the bank.

If the company has chosen to have an automatic link back to its own system the customer is automatically linked back to the company’s own server (i.e. the URL specified in the URL_OK parameter) together with a number of parameters specified below.

Parameter	Data description	Additional information
Orderid	max 10 numerical characters	Unique number that identifies the order.
Butikid	max 16 numerical characters	The unique company code provided by Fspa.
Belopp	max 6 + 2 numerical characters separated by a ’,’	The amount of the transaction. The two last characters after the ‘,’ are ören. The maximum transaction is 10,000 SEK.
Sig	48 characters	The regular checksum produced using the different parameters above.

Figure 5.10. Parameters returned to the marketplace.

The company also needs to be able to later check if a transaction was executed, even if nothing happened during the report back to the company. Therefore are all transactions are stored in a database at FSpa that the company can request data from over the Internet. Such a request is done POSTing the necessary parameters to FSpa and is further described below. The parameters in the forms are of the type “hidden” and the communication is protected by SSL.

Parameter	Data description	Additional information
Ordered	max 10 numerical characters	The unique number that the company want FSpa to check.
Butik-id	max 16 numerical characters	The unique company code.
Sig	48 characters	The regular checksum produced using the different parameters above.

Figure 5.11. Parameters sent to control a transaction.

The response from FSpa comes in a form in a HTML document, which contains the following parameters. The value of these parameters can then be parsed out and checked by the company's own system.

Parameter	**Data description**	**Additional information**
Ordered	max 10 numerical characters	The unique number that the company wanted FSpa to check.
Butikid	max 16 numerical characters	The unique company code.
Belopp	max 6 + 2 numerical characters separated by a ','	Amount of the transaction. If status = 1 (no transaction found) a amount = 'X' will be returned.
Status	max 2 numerical characters	0 = transaction OK. 1 = no transaction with that ordered exist. 2 = the customer interrupted the transaction. 3 = transaction in progress.
Sig	48 characters	The regular checksum produced using the different parameters above.

Figure 5.12. Parameters sent from the bank.

Prices

These are the prices for a company that wants to utilize Föreningssparbanken's service Direct Internet Payment.

• Initial cost:	0 SEK.
• Monthly cost	0 SEK.
• Transaction cost	3 SEK + 2%.

5.3.4 Nordbanken

Requirements on the Internet marketplace

The company needs to have an account in Nordbanken. NB can only make transactions from consumers that are using their Solo service. The Solo service enables the customer to authenticate themselves using a smartcard or a one-time code.

The Internet marketplace needs to install a cryptographic module (called Giroprotector). This module produces a hash value based on the parameters and also a shared secret that is distributed by NB. The input to the Giroprotector is the parameters separated by an ampersand (&). The Giroprotector generates a unique hash code and the first 18 numbers are used as a check that no changes have been made during the transmission.

All communication between the consumer and the bank is protected by SSL.

Payment opportunities.

Nordbanken lets the Internet marketplace offer their customers the possibility to pay in three different ways. Pay direct, Pay later, and by instalment. The first method, Pay direct, means that the transaction is made directly. Pay later means that the transaction commission is held and not paid until the payment day stated by the Internet marketplace. The final payment way is instalment. This means that the transaction can be divided into up to eight instalments.

Payment procedure

The company puts together all necessary parameters and posts them to the bank where a logon page is presented to the customer that wants to perform a transaction. The customer logs in using either a smartcard or a one-time code. If the login is successful the customer is transferred to a page where the transaction information from the company is presented. The customer confirms the payment and is encouraged to follow a link back to the marketplace. If the customer chooses to follow that link the marketplace gets a confirmation of the transaction. Otherwise a check for the transaction has to be done. As seen in the picture below all transaction communication is performed between the consumer and the bank and not via the Internet marketplace.

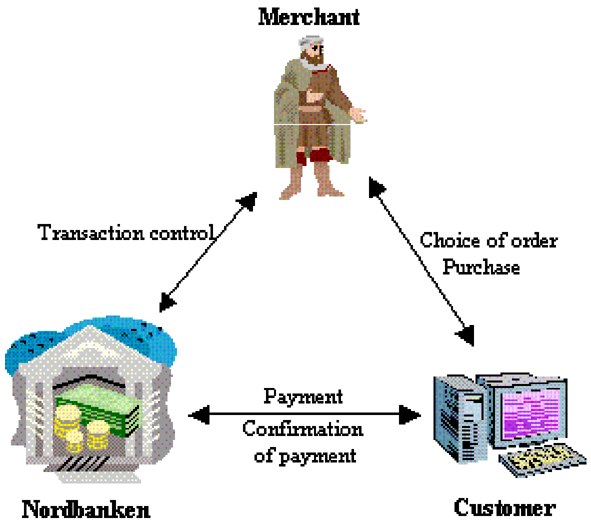


Figure 5.13. The principle of Nordbanken's payment system.

If the customer chooses not to return to the marketplace via the presented link or if the marketplace's server is temporarily down then the marketplace has to check that the transaction actually has been done. This action can be performed in two ways. Via account information or via a service called NB Axess.

The parameters posted by the marketplace are described in the table below. Note that all parameter description in the tables below is taken from Nordbanken's manual [81].

Parameter	**Data description**	**Additional information**
NB_VERSION	4 numerical characters	Version of the payment system.
NB_RCV_ID	9 alpha numerical characters	This code is unique for every company using NBs service Direct Internet Payment. NB provides the number to the company.
NB_STAMP	20 alpha numerical characters	Unique number that identifies the order.
NB_DB_AMOUNT	19 alpha numerical characters	The amount.
NB_DB_CUR	3 alpha numerical characters	Type of currency (only SEK and EUR available today).
NB_DB_REF	25 numerical characters	A reference number used by the Internet marketplace to bind a payment to an order.
NB_RETURN	240 alpha numerical characters	The URL that NB should present to the customer if the transaction was performed successfully.
NB_CANCEL	240 alpha numerical characters	The URL that NB should present if the customer chooses to cancel the transaction.
NB_REJECT	240 alpha numerical characters	The URL that NB should present to the customer if anything goes wrong in the system.
NB_MAC	18 alpha numerical characters	Hash value of selected fields above.

Figure 5.14. Parameters sent to the bank.

When the customer returns to the Internet marketplace by pressing the presented link this information is POSTed via HTTP.

Parameter	**Data description**	**Additional information**
NB_RETURN_STAMP	20 alpha numerical characters	The company's unique code.
NB_RETURN_DB_AMOUNT	19 alpha numerical characters	The amount.
NB_RETURN_DB_CUR	3 alpha numerical characters	Type of currency.
NB_RETURN_DB_REF	25 numerical characters	The reference number.
NB_PAID	26 alpha numerical characters	A transaction number provided by NB.
NB_MAC	18 alpha numerical characters	Hash value of selected fields above.

Figure 5.15. Parameters returned to the marketplace.

The other types of payment methods are using almost the same parameters. These are not described in detailed because they both refer to more traditional sales methods and not the possibility to deliver the goods electronically.

Control of transactions

If the customer chooses not to return to the marketplace after performing the transaction, the marketplace must perform an active control mechanism to verify the transactions. This is done by POSTing a form with the following parameters.

Parameter	**Data description**	**Additional information**
NB_VERSION	20 alpha numerical characters	The company unique code.
NB_RCV_ID	9 alpha numerical characters	The unique transaction code.
NB_STAMP	20 alpha numerical characters	Unique number that identifies the order.
NB_RETURN	240 alpha numerical characters	The URL that NB should present to the customer if the transaction was performed successfully.
NB_MAC	18 alpha numerical characters	Hash value of selected fields above.

Figure 5.16. Parameters posted to control a transaction.

When the bank receives such a form as described above the control system checks the bank's back end system. A form is POSTed to the marketplace with the parameters described below:

Parameter	**Data description**	**Additional information**
NB_VERIFIED	3 alpha numerical characters	The transaction status. Can be YES/NO/ERR.
NB_RETURN_STAMP	20 alpha numerical characters	The unique transaction code requested by the company.
NB_MAC	18 alpha numerical characters	Hash value of selected fields above.

Figure 5.17. Parameters sent to the merchant after control of transaction.

The NB_VERIFIED field can as seen above have three different values. YES means that the transaction has been successfully completed. NO means that the transaction could not be found in the bank's system. Finally ERR means that no correct answer can be given.

Beside these compulsory parameters there can be a number of optional parameters such as currency, reference number and timestamp.

Prices

These are the prices for a company that wants to utilize Nordbanken’s service Direct Internet Payment. These prices include exposure on the bank’s own Internet marketplace called the SOLO market.

• Initial cost:	2000 SEK.
• Monthly cost	150 SEK.
• Transaction cost	3 SEK.

5.4 Micropayments

Some define the term micropayments as low-value electronic financial transactions. What the word low-value actually means, usually depends rather heavily on the micropayment system in question. Generally, the value of an individual micropayment range from as little as a fraction of a cent to a few dollars.

Provision of content is one of the main attractions and benefits of the Internet. Today the majority intangible goods and services on the Internet, information and immaterial resources, are given away for free by most content providers. That because the price on the transaction is often much higher than the actual price of the service itself. To gain some kind of profit for the digital products the merchants often sell advertisement space to other companies. The advertisement on the websites decreases the quality of service given to the user or customer.

5.4.1 Jalda

Ericsson started the development of Jalda and EHPT acquired the technology. EHPT is a joint venture between Ericsson and Hewlett Packard.

Jalda [82] is a standard for open and secure e-commerce on the market that can be used for a wide range of solutions from gaming and music to e- and m-commerce. It consists of a set of APIs and a payment server called SafeTrader. The APIs are offered as freeware. Every customer using Jalda is assigned a special account located at a Payment Provider – a trusted third part, which handles all transactions. Jalda can handle payments from any device with Internet access; from stationary PCs to mobile phones. The merchants can choose to charge the customers by whatever parameter the service or product desires, including elapsed time, quantities, items, mouse clicks, data files, searches or points. All this makes Jalda a sophisticated micropayment system, which enables the merchants to charge the consumer for even very small amount of money.

To secure the transmission concerning the transaction, Jalda uses SSL, RSA for authentication and 3DES for the symmetric encryption. That means that Jalda uses a PKI system for authentication of the symmetric keys. Jalda is a mixture of an account-based and a token-based payment system where the user has to make a pre-payment into an account before being able to buy digital goods, etc. To prevent having the customer send his or her credit card number over the net every time a payment into the account is made, Jalda takes advantage of the use of digital certificates. Therefore, when the user has registered his or her card number at the payment provider the customer receives a certificate which is used instead of the card number when communicating with the payment provider.

Jalda is not bound to the fixed Internet, but can also be used in the wireless world. The wireless Jalda is today based on SMS, but development towards the use of WAP is on its way.

The Jalda payment infrastructure consists of three main parties: the payment provider, the content provider, and of course the customer.

- **Internet Payment Provider (IPP).**
  The IPP maintains the payment server to deliver a secure, trustworthy payment service for consumers and content providers. The IPP might be a bank, a credit card company, an ISP, or a network operator.
- **Internet Content Provider.**
  Content providers are the Internet merchants who provide electronic or physical goods and services such as web shops, mobile services, financial services, etc. The merchants have to implement the Jalda API in their existing solutions to make it communicate with the payment server.
- **Consumer.**
  The consumer can be a regular Internet or mobile phone user. The user has just one account at his / her payment provider and can from that account purchase digital merchandise from all content providers with an agreement with that particular payment provider.

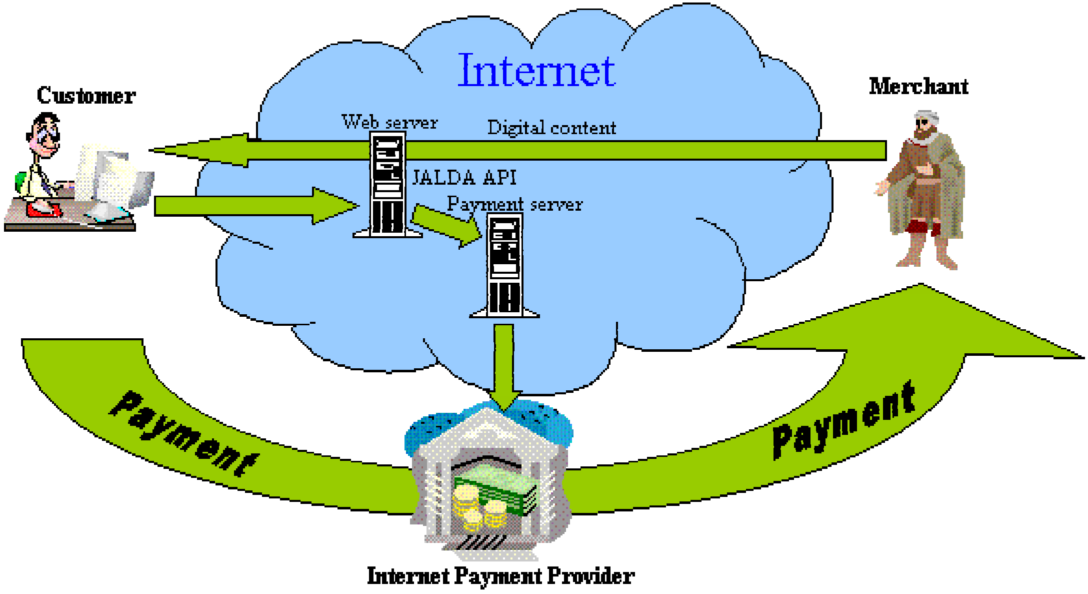


Figure 5.18. Description of Jalda.

When a payment transaction is initiated, the consumer signs an agreement outlining the relevant contractual terms, including cost, the service the customer is buying, time, date, etc. Once the agreement is signed and the IPP notified, the application sends so called “ticks” over the secure connection between the user’s application and the payment server. These “ticks” are the way the services’ charges is being measured and their values are set in advance by the content providers.

The Jalda API is available in both Java and C. The API is simple to implement and only includes four main classes that is used in the content provider’s applications.

5.5 Special payment solutions

5.5.1 Telia Säker Handel

Telia Säker Handel developed by Telia Electronic Commerce is a way for the merchant to offer a complete payment solution to its customers. With this service the merchant enables the consumer to choose whether he or she would like to pay through an Internet bank, with credit cards, have it sent cash on delivery, or by invoice.

The customer needs to accept a digital certificate provided by Telia when choosing to purchase a product. That is to ensure that it is really Telia the customer is communicating with.

The following payment methods are currently available through Telia Säker Handel. The merchant can choose which methods he wants or does not wants to be included in the service offering his customers:

- **Direct payment through the consumer's Internet bank.**
  The available banks are Nordbanken, Handelsbanken, Föreningssparbanken, and SEB. The customer will be directly linked from the merchant's web page into his or her Internet bank, where the payment is waiting to be signed by the customer. After signing, the merchant's account is immediately credited and the delivery of the product can begin.
- **Payment through credit, debit and bank cards with authentication.**
  The available cards are VISA, and MasterCard. This authentication card method only works with cards issued in Sweden. To be able to pay with cards in a authenticated way the consumer needs to apply for a personal signature code, which has the purpose of connecting the consumer to the card. The signature code is sent to the home address of the cardholder. When the customer chooses to buy a product using a credit card, only the signature code needs to be transferred over the net.
- **Payment through credit, debit, and bank cards.**
  The available cards are VISA and MasterCard. When confirming the purchase the user enters just the card number, and expiry date to fulfil the purchase. The transfer of the information is protected by SSL.
- **Cash on delivery.**
  The consumer pays for the product when he or she physically gets it.
- **Pay by invoice.**
  The consumer pays according to the conditions and rules stipulated on the invoice after receiving the product.

Figure 5.1 [83] shows the price in SEK for the different services available in the Telia Säker Handel package:

Basic service	**Initial fee**	**Monthly fee**	**Transaction fee**
Telia Säker handel	5,000	2,000	8
Additional services			
Pay with cards			
Cards with authentication (Swedish VISA and MC)	0	0	

Foreign cards	2,000	0	
Internet bank			
SEB	2,000	0	
Föreningssparbanken	2,000	0	
Nordbanken	2,000	0	
Handelsbanken	2,000	0	

Figure 5.19. Pricesin SEK for Telia Säker Handel.

5.5.2 Telia PayIT

Telia PayIT developed by Telia Financial Services is a payment product which takes advantage of the existence of the user's phone bill or a prepaid user account. Everything the customer chooses to purchase will end up as part of the standard Telia phone bill or in the prepaid account case withdrawn from it. Telia has chosen to only handle products which can be immediately and digitally delivered to the customer. That is because they want to make the trade as safe as possible for all parties; both the merchant and the customer. Telia PayIT also supports charging the customer for clicks or per time units used in the system.

As mentioned above, there are two different versions of Telia PayIT; phone bill and account. The first version is based on the eCharge platform and the second version on the Jalda platform and they have different possibilities and limitations due to the fact that they are based on completely different techniques.

Telia PayIT telephone bill exists in a live version, but the account version is in a pilot test stage. A mobile solution is planned to be out on the market at the end of the year.

5.5.2.1 Version 1.0 eCharge

The eCharge system is based on the existing infrastructure of 900-numbers. Everyone connected to a Telia telephone subscription and also having access to a modem dial-up connection can purchase a digital commodity directly from the web. That means that about 2 million Swedes have access to this kind of payment method. All products purchased will be separately noted on the customer's telephone bill.

The registration for the service is made through the telephone number and the consumer does not have to reveal sensitive information like social security number, credit card information, etc.

A transaction consist of the following steps:

- The consumer finds a product and clicks the 'Telia PayIT' icon to purchase it.
- The digital product is encrypted and transferred to the customer.
- The customer's modem logs off from the Internet and automatically makes a telephone call to a 900-number, and it is this call which is registered by Telia and generates the amount that will appear on the customer's next telephone bill.
- The encrypted product is decrypted and can now be viewed by the customer. The purchase is completed.

Telia PayIT works with analogue and ISDN modems. There are no special programs that the customer needs. Because the customer is already a registered telephone subscriber, no further registration is needed.

To implement Telia PayIT, the merchant needs to retrieve a special user-id and password before starting to add the products which will be included in the range of commodities offered on the web. The merchant adds the desired products to Telia PayIT's special service site.

Every month Telia credits the merchant's account with the amount of money earned from the customers.

5.5.2.2 Version 2.0 Jalda

This, the account version of PayIT uses the open standard Jalda, developed by EHPT. It is based on a prepaid virtually account. The account can be refilled by either taking advantage of the user's telephone bill or using a post-/bankgiro. The consumer registers online and can start purchasing digital goods directly afterwards. In the registration process the customers retrieves a digital certificate which can be used on any computer of the customer's choice.

To use this version of the PayIT system the merchant is required to implement Jalda API in the applications which should be used in debiting the customer. The Jalda API also needs to be implemented to let the merchant communicate with the SafeTrader payment server. The merchant has to register an account at the Payment Provider, in this case Telia. The merchant's account is credit directly after the Payment Provider has registered the purchase.

5.5.3 Telia Advance 900

A 900-number is a regular charge number, where the owner of the number in advance can choose the minute rate and / or a fixed cost that the caller has to pay.

The customer calls a specific 900-number and the cost for it will appear on the next telephone bill. When the 900-number is dialled, a Telia voice informs the caller of the price and rate for that specific call and the customer has a 10 second time period to change his mind and hang up without being charged.

The merchant has the possibility to introduce a computerized call centre to the service with a touch-tone functionality bound to a merchant database, which can store vital information regarding the caller. This can be information such as social security number, access codes, etc.

The merchant will be credited by Telia once a month with the money earned from the customers calling the number. Telia takes full responsibility for the complete payment process: invoicing, monitoring, etc.

The 900-number can only be reached from a telephone connected to Telia's standard telephony net and therefore it can not be reach from any mobile phone.

Either a fixed cost per call or a minute rate per call can be chosen for each 900-number. The maximum charge for both is 200 SEK. Telia take a fee from the merchant of 15% of the total call cost plus 1.25 SEK per minute. A deposit of 30,000 SEK has to be paid by the merchant when registering for the service. The merchant also needs to have a monthly turnover of more than 2000 SEK.

5.5.4 Sonera mobile pay

Sonera mobile pay is a daughter company to the Finish company Sonera (both a smartcard issuer and mobile operator). Their product makes it possible for a consumer to purchase a variety of different products using their standard mobile phones.

Payment methods
The customer pays for his selection via the phone bill. In the future Sonera plans to offer the consumer the possibility to be able to choose from a selection of various payment methods. For example, the consumer shall have the opportunity to direct the payment from his bank account, credit card, or similar. [84]

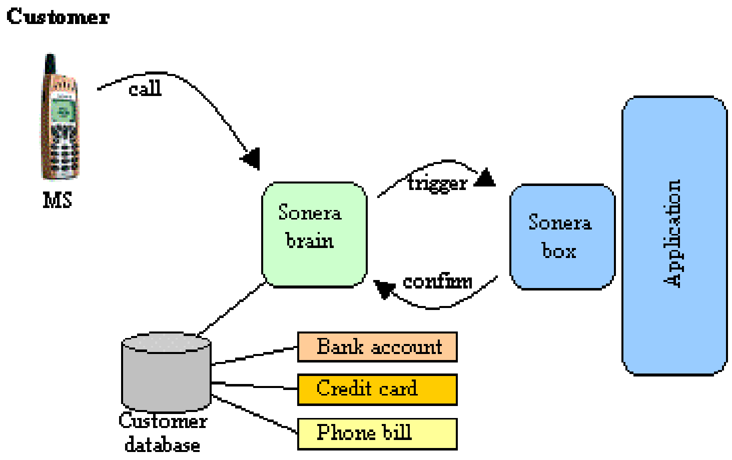


Figure 5.20. Schematic picture of the future Sonera Mobile Pay system.

5.5.4.1 *Example of products*

The Sonera mobile pay has been implemented in several products as shown by the examples below.

Pepsi vending machine
By calling the service number situated on the vending machine the consumer gets a soft drink and is charged for it on their mobile phone bill.

Ticket machine
The consumer chooses between three different service numbers. These numbers gives him three different tickets that are worth different amounts (10, 20, or 40 FIM). The tickets are then valid for three hours and the consumer can choose to buy whatever he wants from some cafés. The tickets are charged on the consumer’s mobile phone bill.

Web surfing
The consumer dials a number on the screen and thereby buys Internet access time for 10 minutes. The Internet surfing cost is charged to the consumer’s mobile phone bill.

Parking
By calling a special number when arriving and then calling another special number when leaving the parking lot the consumer will pay for the exact time he actually used the parking lot. The parking cost is charged to the consumer’s mobile phone bill.

5.5.4.2 *Zed portal*

Sonera offers a media portal called Zed. It is only available to finish customers. The Zed portal gives the user the possibility to download different ringing tones, icons, or compose his own tune using the Java based piano, etc. The consumer can also order up to date information in different areas and get them delivered as SMS messages to his mobile phone. All Zed services are billed on the customer's mobile phone bill.

5.6 Payment hotels

5.6.1 DebiTech

DebiTech AB was set up in Sweden in 1997. It offers several different solutions. They all have in common that the consumer does not need to download or install any Plug-in modules or other software packages. DebiTech also does not require any special hardware such as Digipass or card readers. All that the customer sees is a user-friendly form. The Internet store does not need to invest in any special hardware. [85]

5.6.1.1 *DebiTech Web*

The owner of the Internet marketplace gains access to the payment service through an administration interface over the Internet. Therefore the DebiTech Web does not require any installation, i.e. no hardware or any other specific software package.

When an order is placed on the customer’s website, the consumer is linked from the marketplace into the payment page (made by the marketplace’s own web designers) that is situated on the DebiTech Payment Gateway.

This way the customer does not have to be aware that there has been a change of server. When consumers have completed their payment, i.e. entered their credit card number, expiry data, etc, they are linked back to the marketplace’s web server.

5.6.1.2 *DebiTech Server*

The DebiTech Server is a software package implemented on the marketplace’s server. That means that the consumer never leaves the marketplace to make a payment. The software supports Windows (.com objects), Solaris, and Linux.

All communication between the Internet store and the DebiTech Payment Gateway takes place via an encrypted socket or via an SSL encrypted http header.

DebiTech offers the service Direct Internet Payment with three of the largest banks in Sweden; Föreningssparbanken, Nordbanken, and SEB. The same service is also available for customers in Östgötabanken.

Important partners are IBM in the technical area and National Westminster Bank in the banking area.

DebiTech supports both real SET transactions, where the user has to authenticate himself with a proper certificate and the less secure method called MIA where only the marketplace and the bank have to authenticate themselves to each other. The supported cards are listed below.

Credit Cards:
Master Card
VISA
American Express
Switch
Dancard
Diners
JBC
Eurocard

SET:
Master Card
VISA
Eurocard

Figure 5.22. Supported cards.

The charging is based on the fact that the Internet marketplace has an account at DebiTech. The charging model is described below:

- **Start cost:** 25,000 SEK.
- **Monthly fee:** 50 SEK / month.
- **Internet Direktbetalningar:** 3 SEK / transaction + every bank’s own costs.
- **Credit card cost:** 4% of the transaction value (turnover up to 1M SEK a year) (a lower percentage with higher turnovers. Minimum is 2.8%).

5.6.2 KLELine

KLELine was created as a financial institution in 1996 and is headquartered in Paris, France with offices in New York and London. KLELine is a subsidiary of BNP-Paribas, Europe's third largest bank group. [86] KLELine offers complete payment solutions to merchants and customers throughout the world.

For the customers:

- Payment via a virtual wallet, (K-Wallet). K-Wallet is a Web-based secure payment service allowing customers to pay for purchases in an easy way.
- Payment by credit or debit card using a secure connection. Security is ensured by an integration of a 40 to 128 bits SSL key and a 512-bit RSA encryption.

5.6.3 NetGiro

Netgiro was founded in 1997 and the head office is located in Sikla, just outside Stockholm. They offer a complete suite of payment methods for their customers. By implementing their API (available in JAVA, C or .com) their customers get a quick start of their e-business. [87]

5.6.3.1 NetGiro Transaction System

Netgiro's transaction system, Netgiro TS, is the heart of the operation. It offers a global solution for multi-bank and multi-currency functionality with a universal merchant interface, digital payments, billing, clearing, and settlements.

The NetGiro transaction system mechanism can be described as follows. When the consumer places an order, the communication to the Internet marketplace is protected by a 128-bit SSL encryption. The Internet marketplace then contacts the NetGiro TS and the customer’s payment information is sent to the NetGiro server. Thereafter, all transactions towards the chosen financial partner is handled by NetGiro. The funds are then transferred to the marketplace’s bank account. Every reported transaction is linked to an order reference. This allows the marketplace to match the billing information with payments received through the NetGiro TS.

Netgiro offers the service Direct Internet Payment with two of the largest banks in Sweden: Föreningssparbanken and Nordbanken, and is negotiating with SEB.

They have contacts with several international banks, for example in France. Therefore NetGiro offers their customers a multi currency payment system. This means that their customers can trade in a choice of currencies and settle into a different currency. In real life this means that one can sell merchandise in for example US dollars and German Marks and settle from a Swedish kronor bank account.

Aside the contract with NetGiro the customer also has to establish a card redemption agreement to be able to perform credit cards transactions. Right now NetGiro is negotiating with Östgötabanken to be able to offer their customers the ability to establish only one single contract if the customer chooses to use Östgötabanken as its card redempter.

NetGiro supports both real SET transactions where the user has to authenticate himself with a proper certificate and they also supports the less secure method called MIA where only the Internet marketplace and the bank have to authenticate themselves to each other. An interesting aspect is that Martin Fransson, sales manager Nordic, claims that their fraud-rate is less than 1% all over Europe. The supported cards are listed below.

Credit Cards:
Master Card
VISA
American Express
Switch Card
Dancard
Diners
Carte Bleu

SET:
Master Card
VISA
American Express

Figure 5.21. Supported cards.

5.6.4 SecureTrading

SecureTrading was founded in 1995 and is situated in the United Kingdom (northern Wales and London). The company provides the marketplace with a so called 'plug and play' solution for processing payments. SecureTrading operates a network of gateways with direct links to the banks. This means that the payments that the marketplace has received are authorised instantly and are immediately available for payment into the marketplace’s bank account. SecureTrading is able to offer its customers the possibility to implement a multi currency payment system. [88]

The security aspects of the solution provided by SecureTrading are digital signatures or certificates. Digital signatures are used throughout the system in order to ensure that transactions arriving at a gateway are from an identifiable marketplace, and that any information passed back to the marketplace is from a SecureTrading gateway. As usual each signature uniquely identifies its source. Gateways also communicate with each other and with the control system using such digital signatures. In the event that a merchant's digital signature becomes a security risk in any way, the digital signature is immediately revoked and will no longer function within the system. SecureTrading is the official CA for these digital signatures.

An appealing security aspect of the SecureTrading solution is that in their system they are using IPSec to tunnel all traffic. All communication within the system is strongly encrypted using 2048-bit RSA encryption with variable 168-bit session keys.

Since this is not a Swedish based company their attitude towards credit cards are a little bit different. Outside Scandinavia people are, as mentioned before, more willing to give out their credit card number on the Internet or even on the telephone. Still SecureTrading claims that their system is even more secure than SET since it uses stronger encryption and longer session keys. However, they are not able to authenticate the credit card owner in any way. The supported cards are listed below.

Credit Cards:
Master Card
VISA
American Express
Switch
Solo
Discovery
JCB

Figure 5.23. Supported cards.

The charging structure is set up by two components:

- Annual Fee (currently £195 plus VAT).
- Transaction fee based upon transactions processed.

The basic transaction fee is 1.5% on authorised transactions (failed transactions, refunds, etc. are not charged) plus a £10 per month minimum.

Since the company Ananas.net, owned by Celltribe, is using SecureTrading services right now, Ian Musselwhite, was able to inform us that about 5-7% of their commission is paid in credit card transactions.

5.7 Some merchants and their payment solutions

The table below shows a number of Swedish companies that uses some kind of payment method. Celltribe's competitors (chapter 7) are also included in the table even if some of them do not have a working payment system running.

Telia Säker Handel	www.noll7noll.com, Telia Refill
Netgiro	SJ, SF bio, sportus.se, boxman
Debitech	Swedetown.com, www.livingbody.com
KleLine	Iobox
Unknown	Goyada
N/A	Halebop
Unknown	Comviq
SecureTrading	Ananas

Figure 5.24. Merchants' payment solutions.

5.8 Alternative payment methods

When thinking about paying for merchandise or services one usually thinks about cash or perhaps credit cards. The most common, at least in Sweden, is still paying using cash. Since this does not work on the Internet the Swedish banks have developed a service called Direct Internet Payment (section 5.3). Another possible payment method is using credit card in a more or less secure way. In the ever-changing digital era these methods are not the only ones available. This section presents a number of non-standard payment methods.

5.8.1 Paying with your mobile phone bill

Whether using the Internet in your home via a modem pool or if you are WAPing when waiting for the subway you want to be able to buy both merchandise and value added services. Since the ISP already is measuring your traffic and is billing you for the time spent or maybe in the future for the data sent over the network and sending you a bill every month, there should be a possibility to pay not only for the basic network connection, but you should be able to pay also for these purchases of added services.

For the mobile case, this solution would enable the user to initiate a purchase from practically everywhere in the world as long as the visited country is using the customer’s particular mobile system (GSM for example). This is because roaming is such a well developed service.

The finish company Sonera has a solution called Sonera Mobile Pay that enables the customer to for example buy a soft drink from a vending machine and pay it later on their mobile bill (See section 5.5.4)

An extension of this method of paying with your mobile bill is to be able to pay on different bills. If the network operators could establish contracts with other types of businesses that people are used to get bills from every month. Maybe you want to pay for these services more periodically, for example on your electricity bill or your water bill that you are sent every quarter. This of course means that a lot of different data systems need to be integrated.

5.8.2 Paying automatically from your bank account

If a secure authentication scheme could be developed the most natural way is paying with money from your regular bank account. This of course demands a secure authentication method.

5.8.3 Paying via invoice

When a purchase of any kind is made the company offering the product could in some way register the user who performed the purchase. If the address could be retrieved from for example from some authority (i.e. ‘Folkbokföringen’ in Sweden) maybe with help from the network operators the actual merchant would be able to send an invoice to the customer. This method is not suitable for small payments unless the users are only invoiced periodically, once a month for example.

5.8.4 Paying with loyalty points

Loyalty points are described in section 3.1.1.1. After earning the necessaty number of loyalty points the user should be able to use them instead of any form of regular or electronic cash. These loyalty systems offer a completely new opportunity. In a distant future there should be a possibility to use different types of loyalty points to pay for different types of services. A trading possibility should exist. It should be possible to exchange for example IKEA points to Beenz that then makes it possible for the user to purchase a certain service.

6 M-commerce enabling technologies

This chapter describes some different communication technologies, which has a possibility to be used as a bearer of m-commerce transactions.

6.1 WAP

The WAP protocol suite [89] is based on the common Internet protocols, but aims to be a light version specially suited for wireless use. If one compares the WAP protocols with the Internet protocols the correlated protocols for HTTP and HTML in the Internet world are the WSP (Wireless Session Protocol) and the WML (Wireless Markup Languages) in the WAP world.

Due to the fact that wired and the wireless nets are using different stacks of protocol, it is not possible to send data directly from a wireless client to a web server situated on the wired Internet. A so called WAP gateway has to be put in between the two networks. The gateway acts as a proxy between the client and the web server, converting the data into the correct protocol suite.

The traffic in the wireless network is binary coded and the WML code is compressed before sent out over the air. The main thought with the WAP protocols is that they should be optimised in such a way that as little data as possible is sent between the client and the gateway.

6.1.1 Gateway/Proxy

The gateway is connected to both the wireless and the wired net and acts as a proxy in both directions.

When the client makes a request for a particular page on the Internet, a WSP request with the specific page’s URL is send to the gateway. The gateway then makes an HTTP request to the web server specified in the URL, acting as a proxy for the client. The web server returns the page to the gateway, which translates it and sends it back to the client, now acting as a proxy for the web server.

The data received by the gateway from the client is binary encoded and therefore has to be decoded before it can be send out over the Internet. The packets have to be changed and therefore every layer of the WAP suite has to be unpacked and the data converted into the Internet protocol suite.

The gateway has other important responsibilities, which ease and speed up the communication. It acts as a DNS server towards the client and also caches static information, which can be reused in later transmissions between client and gateway.

The client and the gateway are aware of each other for a time period even after the connection has broken. This is because static information like phone type, version, etc can be stored and the next time the client tries to establish a connection to the gateway the handshake process will be faster. [90]

6.1.2 WAP bearers in GSM

WAP is independent of which air interface the data is transferred over and therefore supports a lot of different bearers.

The most common bearer in today's WAP phones is SMS (Short Message Service), USSD (Unstructured Supplementary Service Data), and CSD (Circuit Switched Data). [91]

6.1.2.1 SMS – Short Message Service

SMS is a store and forward protocol. That means that no connection is established before the transmission of data and therefore all client specific data has to be sent in each SMS message. The maximum length of a message is 160 characters.

6.1.2.2 USSD – Unstructured Supplementory Service Data

USSD is a session oriented protocol, which means that a connection between the client and gateway is established before sending any data. The connection is active until either the client, the application, or a time-out shuts it down. The maximum length for a message is 182 characters. The protocol uses the same signalling path as SMS, but besides that similarity they have not very much in common. USSD works in a way that all commands given from the mobile client are always routed back to the client's home network, which enables the client to be roaming.

6.1.2.3 CSD – Circuit Switched Data

CSD is the protocol that is most commonly used in today's WAP-services. The protocol establishes a connection between the client and the gateway. Theoretically the setup of the connection takes about 10 seconds in the digital case. If there is not a digital connection all the way, and for instance if an analogue handshake to a modem pool has to be made, the setup of the connection can take up to 30 seconds.

6.1.2.4 GPRS – General Packet Radio Service

GPRS is a packet based bearer and the result is a direct connection without any need for establishing a connection with multiple handshakes, etc. The client is 'always' connected to the gateway. The theoretical maximum transmission speed is 177.2 kbit/s.

Different services can be executed in parallel. For instance a voice call can be held at the same time a WAP-service is executed.

6.1.3 WAP's protocol suite

There are four different alternative modes in which a session can be established. The session can be connection-oriented or connectionless. Either of these cases can be with or without security (authentication and encryption).

In a connectionless session without security both the WTP and the WTLS layer are removed, which means that WSP is directly on top of WDP. In that mode no acknowledgment of received data is sent and therefore there is no guarantee of the transmission, as there is in a connection-oriented session.

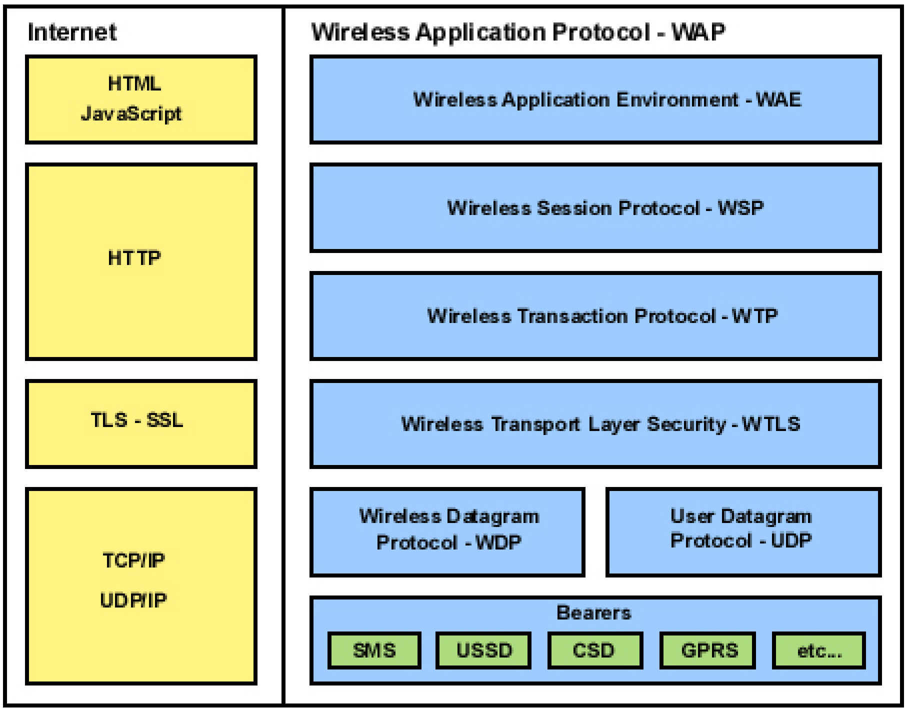

Internet
HTML
JavaScript
HTTP
TLS - SSL
TCP/IP
UDP/IP
Wireless Application Protocol - WAP
Wireless Application Environment - WAE
Wireless Session Protocol - WSP
Wireless Transaction Protocol - WTP
Wireless Transport Layer Security - WTLS
Wireless Datagram Protocol - WDP
User Datagram Protocol - UDP
Bearers
SMS
USSD
CSD
GPRS
etc...

Figure 6.1. The Internet- and WAP protocol stack.

6.1.3.1 WAE – Wireless Application Environment

WAE is the mobile device's user interface. It is designed to be able to host a lot of different applications. To succeed with its task WAE consists of three important components. These components are WML (Wireless Markup Languages), WMLScript, and WTA (Wireless Telephony Application).

6.1.3.2 WSP – Wireless Session Protocol

This layer links WAE directly to the datagram layer in a connectionless session and to the transport layer in a connection-oriented session.

The purpose of this protocol is to establish a session between the mobile client and the gateway. WSP also handles interrupt in the communication as changes of bearer etc. Instead of ending the session after that the last byte has been sent, the session can be suspended and then later be reactivated if more data is to be transported.

WSP is WAP's counter part to Internet's HTTP and is based on HTTP v1.1. The largest different between the two protocols is that WSP is binary encoded. Due to the fact that about 90% of the WSP traffic contains static information, the WSP caches packet headers to avoid sending unnecessary data over the air.

6.1.3.3 WTP – Wireless Transaction Protocol

The WTP protocol is responsible for controlling sent and received packets. The protocol supplies a reliable communication path where each packet is assigned a special identity to be able to prevent packet loss and acceptance of duplicate packets.

There are three different modes in which WTP can be used:

- **Unreliable one-way communication.**
  No acknowledgment of sent data. Lost data cannot be resend.
- **Reliable one-way communication.**

Acknowledgment of sent data. Lost data can be resend.

- **Reliable two-way communication.**
  Acknowledgment is attached to the response. The acknowledgement is hen confirmed and sent back. Lost data can be resend.

The protocol applies pending confirmation on sent data. That means that the receiver waits for a period of time before sending back acknowledgements of received data if the receiver has reason to believe that more data will be sent that also needs to be acknowledged.

6.1.3.4 WTLS – Wireless Transport Layer Security

The purpose of this layer is to provide security for data send over the air (between the mobile client and the WAP gateway). WTLS is based on SSL (Secure Socket Layer) and the later standard TLS (Transport Layer Security) from the Internet protocol suite.

The protocol is optional and need not to be used in the WAP stack. In the setup phase encryption keys are exchanged between the client and the gateway. The protocol encrypts data and supplies authentication using digital certificates.

6.1.3.5 WDP – Wireless Datagram Protocol

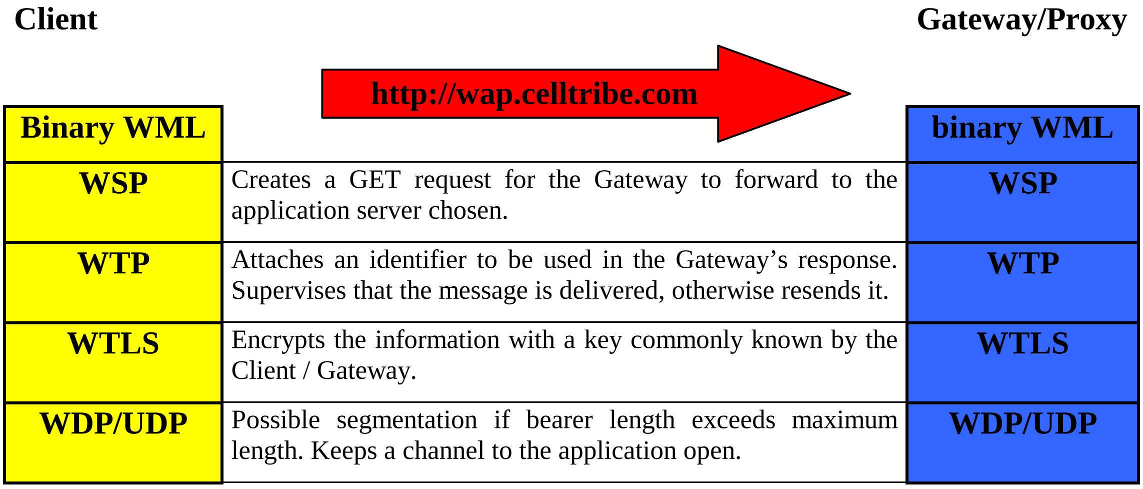
WDP makes WAP independent of which bearer it uses. This layer is only needed when using a bearer that does not support UDP (User Datagram Protocol). For these bearers, WDP takes care of the necessary datagram functionality.

6.1.4 Communication Client – Gateway

The communication between the mobile client and the WAP gateway can (as described in earlier sections) be accomplished both connectionless and connection-oriented with the use or not use of the security layer.

Let us say that the mobile client makes a request for a web page by giving a URL (e.g. http://wap.celltribe.com). The client also wants this connection to be both reliable and secure. The three figures below show in general how the communication between the client and gateway looks like in the different protocols. In this case the gateway acts as a proxy between the client and the content provider (celltribe.com).

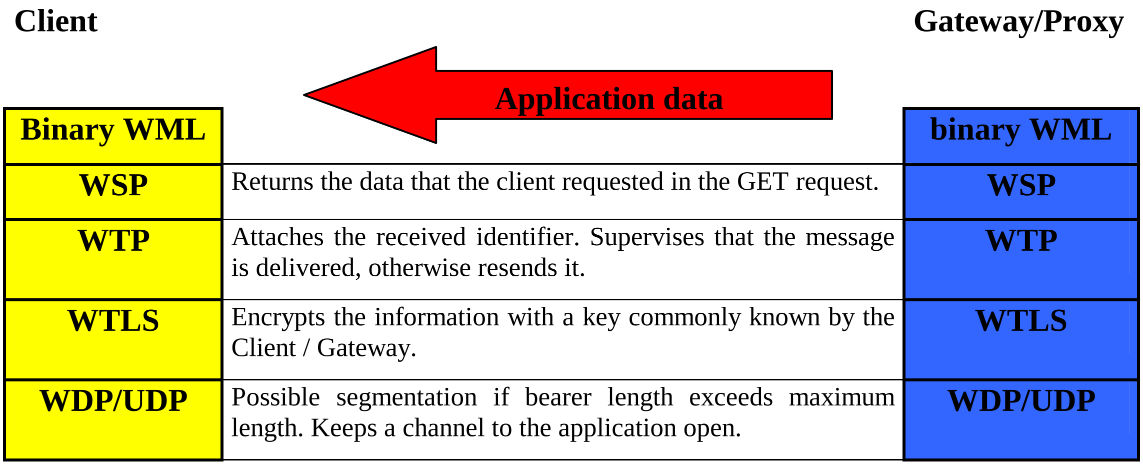
In the first step the client makes a request for the specific document. [92]



Binary WML		binary WML
WSP	Creates a GET request for the Gateway to forward to the application server chosen.	WSP
WTP	Attaches an identifier to be used in the Gateway's response. Supervises that the message is delivered, otherwise resends it.	WTP
WTLS	Encrypts the information with a key commonly known by the Client / Gateway.	WTLS
WDP/UDP	Possible segmentation if bearer length exceeds maximum length. Keeps a channel to the application open.	WDP/UDP

Figure 6.2. Communication between the client and the gateway, first step.

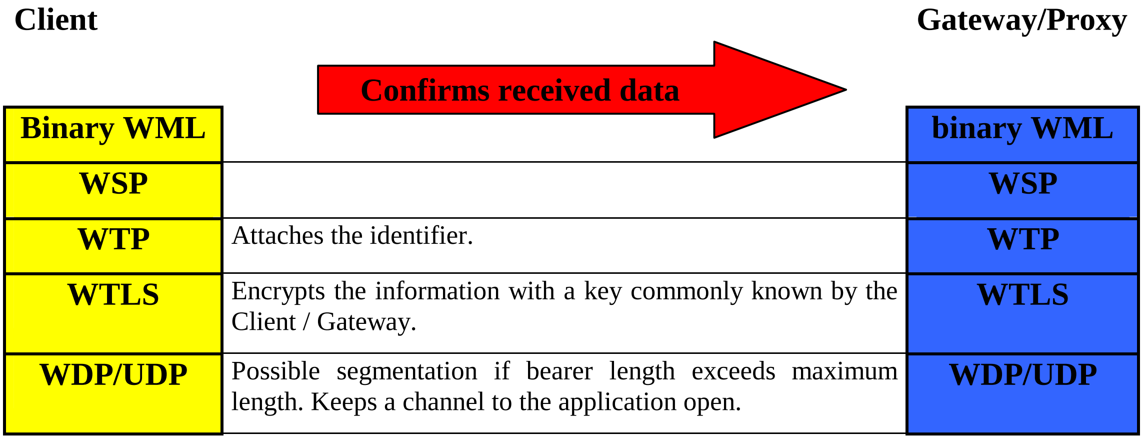
In the second step the gateway answers the client's request by returning the requested document binary encoded to the client.



Client		Gateway/Proxy
Binary WML		binary WML
WSP	Returns the data that the client requested in the GET request.	WSP
WTP	Attaches the received identifier. Supervises that the message is delivered, otherwise resends it.	WTP
WTLS	Encrypts the information with a key commonly known by the Client / Gateway.	WTLS
WDP/UDP	Possible segmentation if bearer length exceeds maximum length. Keeps a channel to the application open.	WDP/UDP

Figure 6.3. Communication between the client and the gateway, second step.

In the third and last step the client sends an acknowledgment back to the gateway saying it has received the requested document.



Client		Gateway/Proxy
Binary WML		binary WML
WSP		WSP
WTP	Attaches the identifier.	WTP
WTLS	Encrypts the information with a key commonly known by the Client / Gateway.	WTLS
WDP/UDP	Possible segmentation if bearer length exceeds maximum length. Keeps a channel to the application open.	WDP/UDP

Figure 6.3. Communication between the client and the gateway, third step.

6.2 GSM

In 1990 the first version of the GSM specifications were published, describing its first phase. Commercial service was started in the middle of 1991, and by 1993 there were 36 GSM networks in 22 countries. Since then GSM has become the largest standard for telecommunications, spreading from Europe to the rest of the world.

6.2.1 Network architecture

The GSM network can be divided into three main parts. The Mobile Station (MS) that is carried by the subscriber, the Base Station Subsystem (BSS) that controls the radio link to the MS, and the network system. It is the network component that is the most advance part. It includes the Mobile Switching Center (MSC) that performs the switching of calls between the mobile and PSTN network. It also handels the management of mobile services.

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). The BTS holds the radio tranceivers, i.e. antennas, that define a cell and handles the radiolink protocols with the MS. The BSC is the connection between the MS and the MSC. It manages the radio resources for one or more BTSs. It handles radiochannel setup, frequency hopping, and handovers etc.

The MSC acts like a switching node between the GSM network and the PSTN or the ISDN net. It also offers all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing.

Their exists two important registers in the GSM system, the Home Location Register (HLR) and the Visitor Location Register (VLR). The HLR contains all the administrative information of each subscriber registered in that GSM network. Also the current location of the MS is found in the HLR. The current location of the MS is in the form of a Mobile Station Roaming Number (MSRN), i.e. an ISDN number. This number is used when routing incoming calls to the proper MSC.

The Visitor Location Register holds selected information about an MS that is currently visiting another area than covered by its HLR. For logical reasons the coverage of a VLR often is the same as for an SMC.

Another important register is the Equipment Identity Register (EIR) that contains a list of all valid mobile equipment connected to the network. This prevent that stolen devices are used in any GSM network in the world. [93]

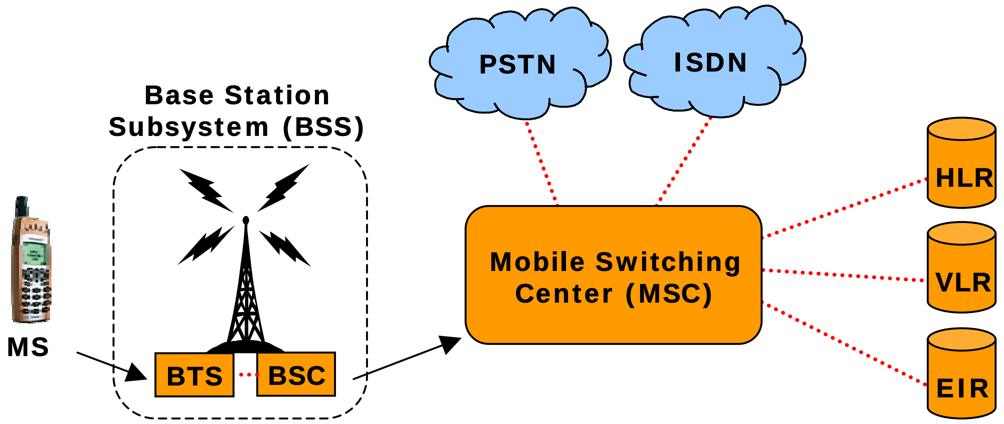


Figure 6.4. Schematic overview of the GSM network architecture.

6.2.2 Techniques

The GSM network utilizes both Time- and Frequency-Division Multiple Access (TDMA/FDMA) to enable multiple users to share the limited radio spectrum. FDMA divides the total 25 MHz bandwidth into 124 carrier frequencies of 200 kHz bandwidth. One or more carrier frequencies are then assigned to each base station. Then TDMA is used to divide these carrier frequencies into eight time slots. One time slot is used for transmission by the MS and one for reception. Of course the uplink and downlink use different frequencies. Each group of eight time slots is called a TDMA frame.

GSM is a digital system, which means that analogue speech signals must be digitalized. The GSM system is using a technique called Pulse Code Modulation (PCM). The GSM network is operating at a frequency of 900 MHz and 1800 MHz.

The supported data rates are 300 bps, 600 bps, 1200 bps, 2400 bps, and 9600 bps. Today even the fastest transmission speed must be considered to be very slow. [94]

6.2.3 SMS

A value added service that was introduced with GSM is the Short Message Service (SMS). The SMS service had no equivalence in the old analogue system. SMS is a store and forward protocol, which means that no connection is established before the transmission of data and therefore all client specific data has to be sent in each SMS message. SMS is a bidirectional service for sending short alphanumeric (up to 160 bytes, one byte equals one character) messages. For point-to-point SMS, a message can be sent to another subscriber to the service, and an acknowledgement of receipt is provided to the sender. SMS can also be used in a cell-broadcast mode, for sending messages such as traffic updates or news updates. Messages can be stored in the SIM card for later retrieval. [95] Some phone manufactures have made improvements to the SMS standard. For example using Nokia’s SmartSMS the user can update the phone’s ringing tones and logotypes. [96]

6.3 GPRS

GPRS stands for General Packet Radio Service and is a standard recommended by ETSI (European Telecommunications Standard Institute) [97] to be the next development for data communication in today’s GSM networks. This is an important step towards the third generation mobile networks UMTS. The system is being implemented in certain areas throughout the world. GPRS is thus an enhancement of the existing GSM architecture and will exist in parallel and will also improve the bandwidth available for the user.

The most important different between GSM and GPRS is that the later is a packet-switched system. This means that no circuit switched connection needs to be established between the sender and the receiver. Nevertheless it uses the existing GSM system for normal speech. Thus Voice over IP is not a part of GPRS. In today’s GSM network data is transferred as any normal conversation, a full duplex channel is established between the sender and the receiver. Therefore a significant amount of bandwidth is used for sending nothing. With the introduction of GPRS the data communication is separated from the ordinary voice communication at the base station. The ordinary voice communication is sent through the standard GSM network and the data communication is sent through a packet-switched network. As seen in figure 6.4: [98]

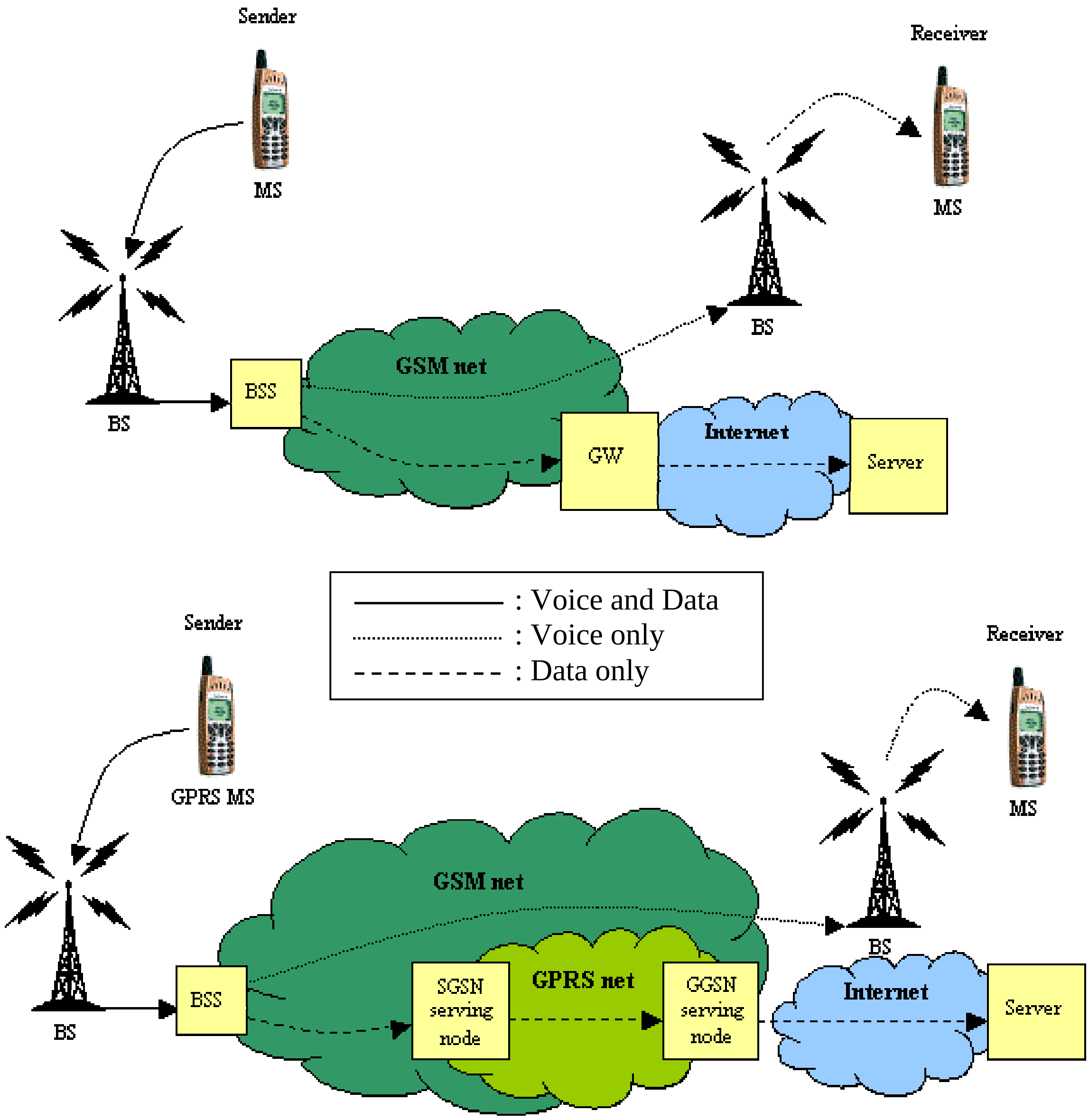


Figure 6.5. GPRS improvement.

In today's GSM system the data communication rate is 9.6 kbit/s. With the introduction of GPRS a theoretical maximum communication rate of 177.2 kbit/s could be achieved. Nevertheless this is theoretical value that is hard to achieve in a practical environment. In practical implementations the transmission rate is expected to be around 40 kbit/s. GPRS achieves this improved bandwidth by dynamically allocating timeslots. If all timeslots are available the user will achieve a high communication rate but if many users are sending data or making voice calls at the same time the communication rate will be much lower.

Even if the improved data communication rate is an important upgrade the most important issue is that the user can be online all the time and yet only pays for the data that he actually sends.

Another important feature with GPRS is that the network operators are able to implement the new GPRS nodes gradually. Therefore the new GPRS technique can first be implemented in areas with lots of data communication (typically large cities). This is achieved because of the way that GPRS dynamically allocates the radio channels. GPRS will support both connectionless communication (typically the IP protocol) and connection oriented communication (typically X.25). The new GPRS nodes that are inserted into the GSM network are called Servicing GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN).

A great feature of GPRS is that it supports IP communication. This means that the Internet protocol stack can be used all the way to the mobile device. Each mobile phone is identified with a unique Packet Data Protocol address (PDP). The format of these PDP addresses is chosen by the network operator. It can for example be an IPv4, IPv6, or X.25. [99]

6.3.1 Mobile phones

As GPRS will exist in parallel with the GSM system all existing mobile phones will continue to work as usual for ordinary voice communication. These users will not be able to benefit from the advantages of the new GPRS service. New GPRS enabled phones will be needed in order to use these new features. GPRS phones that are or will be available to the market is for example, Motorola’s Timeport P7389i and Ericsson’s R520.

6.3.2 Time to market

British Telecom started to introduce GPRS in its network during the summer of 2000. This introduction is focused on business clients and is mainly implemented in the southern parts of the country. Motorola is the only phone manufacturer that actually has GPRS telephones out on the market. Users who want to take advantage of the GPRS services are forced to get a GPRS phone. Towards the end of the last quarter of the year 2000 British Telecom is planning to offer their GPRS services all over the country and to private subscribers.

The Swedish market is a little bit behind. Nevertheless all three Swedish mobile operators, Telia, Tele2 (Comviq), and Europolitan, are implementing the GPRS nodes into their GSM systems. All these three actors plan to launch their GPRS services in the beginning of next year. As in Great Britain the GPRS services will first be offered to business customers.

As the GPRS network demands that the customers invest in new mobile phones the actually take off for the use of GPRS is expected to be a couple of years in the future. As described in section 4.6 GPRS is not expected to significantly penetrate the market until the year of 2003. [100]

6.4 Computer Telephone Integration

An alternative to the obvious channels (like WAP and Internet) is a classical method called touch-tone. The user calls a number and is then transported through voice messaging system by choosing different alternatives by pressing buttons on the phone.

This interaction between the user and a switchboard can then be connected to the company’s existing data system, interacting with different applications and accessing databases. In most touch-tone systems there exist even more opportunities like ordering information which is delivered via fax or to talk live with a telephonist who instantly knows all data the user has given in the touch-tone dialogue and interconnection with data from databases bound to the service. All these activities are typically categorized as Computer Telephony (CT) and can be defined as the technique of coordinating the actions of telephone and computer systems, Computer Telephone Integration (CTI).

If a company is interested in utilizing a touch-tone system there are three main alternatives. The basis is a card that is inserted into a dedicated computer connected to the existing switchboard. This card is provided by for example Dialogic. The card can, if needed, be programmed in C. This is considered to be a pretty demanding task. The alternative is to first invest in the switchboard card and then also invest in a software product from a company called Envox. Their software makes it easy to program the switchboard card using a comprehensive graphical tool that makes it easy to design the structure of the touch-tone menu system. The third alternative is to specify how the entire service should work and then let a third party implement the solution including the dialogue. This can be done by contacting a company such as Objecta, who has delivered several touch-tone call-centres and call queuing systems to Swedish banks. [101]

6.4.1 Benefits for the company

The benefits for the company are several. First of all it is a new channel for their customer to get in touch with the company. Further more there exists several positive aspects of installing a touch-tone system.

- Constant availability. 7 days a week 24 hours a day.
- Customer care personal do not have to deal with standard questions.
- Routine procedures are executed at a low cost.

6.5 SIM cards

6.5.1 SmartCards

There are lots of cards that go under the name smartcard. The concept ranges from regular SIM cards with normal contacts to advanced cards with built in microprocessors and antennas with RF-communication. In this report, when speaking of smartcards what is meant is a SIM card with a microprocessor containing the same three elements as a standard computer: a processing unit (CPU), memory for data storage (EEPROM, RAM, ROM, FLASH), and the opportunity to control input and output data (operating system).

Since the processor is quite weak, a complicated calculation can take a relative long time to execute. The memory on the newest cards is around 32kbytes, which means that the application has to be very small and code optimised for space. Even though both processing power and memory size is expected to grow in the future, these parameters will always be considered small compared to the typical desktop computer. Another thing that makes code optimisation necessary is the limited power supply that almost always is a factor when discussing products that are going to be in mobile devices.

An important issue discussing smartcards is the fact that the information on them is being stored both to avoid damage and theft. An essential advantage for smart cards compared to other classical storage mediums like for example magnetic stripe cards, which store their information on the outside of the card and can be easily copied, is that the smart card is tamper resistant. Today smart cards must be considered to offer a modest security level. They are often a medium for storing such confidential information such as private keys, account numbers, shared secrets,, or passwords. Another procedure that is ideal to take place on the smart card is different security operations such as encryption and producing of unique hash values. Several of the more advanced smartcards support the most common symmetric and asymmetric algorithms, 3DES and RSA. To be able to use the RSA algorithm with reasonable speed a co-processor is usually necessary because of the heavy computation that is needed.

There are quite a few vendors in on this market. For example GemPlus, Schlumberger, and ID2 should be mentioned. They all are major actors in this area and offer a great variety of different kinds of cards.

Figure 6.6. Smartcard.

6.5.2 Electronic Identity Card

The purpose of the Electronic Identity Card (EID) [102] is to clearly, without any doubts, identify the cardholder. It will have the same function as a regular identity card (i.e. driving licence), but will be used in the digital world in analogous to regular ID cards.

The EID card shall support three basic services:

- Strong user authentication.
- Confidentially for messages and communication using encryption.
- Digital signatures for message authentication, data integrity and non-repudiation.

In e-commerce this means that the buyer using his/her digital signature will be legally bound to his/her every electronic commitment. The card employs digital technology to secure digital information in analogy with the way that ordinary paper documents are secured by physical envelopes, seals, and hand-written signatures. [103]

The EID card is a smartcard with a temper resistant memory containing private cryptographic keys and digital certificates related to these keys. The certificates contain the following:

- The identity of the cardholder.
- Public key corresponding to a private key stored on the EID card.
- Certificate issuer.
- Certificate policy.

Other more sensitive information like full name, social security number, citizenship etc. may also be included in the certificates.

The private keys stored in the EID are only used internally on the card. Because the keys never are exposed outside the card it is impossible for a hacker or evil software to capture the keys.

To activate the card a PIN code, known only to the rightful cardholder, has to be entered. After a number of unsuccessful trials the card will block itself from further use.

6.5.3 SIM Application Toolkit

SIM Application Toolkit (SAT) is used for value added services and e-commerce using GSM phones to do the transactions. The first draft documents were specified in 1995 from the work and result of SMG9. This resulted 1996 in the ETSI standard GSM 11.14.

This standard could for instance enable the user to check his/her bank account and pay bills using a SAT enabled phone with an appropriate SIM Toolkit-specific SIM card. This card will provide much of the intelligence to perform a transaction over GSM. An important function that is of great advance for the SIM Application Toolkit is that the SIM card can contain user specific information. This unique personal information allows security-related functions and identity verification to be carried out, which of course is extremely essential for electronic commerce.

Another important factor with the SIM Application Toolkit is that it is possible to update the SIM over the air (OTA). This makes it possible to both alter existing services and even download completely new services to the user. In the current standard SMS is used as a bearer for this updating procedure. [104]

The SAT programmed into the special GSM SIM card essentially enables the SIM card to control and drive the GSM handset interface. SAT can build up an interactive exchange between a network application and an end user and access or control access to the network. This means that the SIM card takes a proactive role in the handset, which means that that the SIM can initiate commands independently of the handset and the network.

The SAT standard is a client-server application that offers a set of commands that are sent from the SIM card to the handset or the network. On the handset’s screen it looks like a series if menus, where each item in the menu is linked to a command or a set of commands in the toolbox.

Today all larger mobile manufacturers have phone models that support the SAT. The most recent models from Ericsson (T18s, T28s) and Nokia (3210, 7110, 8850) are all SAT enabled devices. The third major phone manufacturer, Motorala, have also some SAT enabled devices and their main product, the Startac model, can be upgraded to operate with the SAT standard. [105]

7 CellTribe’s Competitors

This chapter looks at some of Celltribe’s nearest competitors, investigating if they are using any payment system and in that case how they have solved the payments.

There are a few competitors in Sweden to Celltribe in making mobile portals. The major ones are Goyada, Halebop, Iobox, and Room33. The only services of interest in this report is if the competitors have implemented any payment system and in that case how it works. Also worth noticing is if they offer their costumers the ability to reload their mobile refill card, and how they have solved the communication with the issuers, i.e. the operators Comviq, Telia, and Europolitan.

7.1 Goyada

The services Goyada are offering their customers are a few information services like weather, stocks, and news reports. They also have services like best price on CD’s and the quote of the day. [106]

Goyada has their own portal currency called YadaCash, which is used internally in the portal to let the customers pay for services such as having a news SMS sent to their mobile phones. The only present way to refill the YadaCash account is to recruit new members and perform different services in the portal. The customers do not have the option to make a payment to gain more YadaCash, although Goyada has the possibility of arranging for such an exchange system. That is because they already offer their customers the ability to reload their mobile phone refill cards through different kinds of payments methods.

The customers can reload their Comviq, Telia, and Europolitan refill cards. Goyada does not have a digital solution to the communication with the operators and can therefore not receive the codes in digital form. That means that Goyada acts like a normal retailer and manually enters the reload codes from the paper certificates into their database. The payment methods they are currently offering their customers are:

- **Direct transaction from an Internet bank.**
  Nordbanken, Handelsbanken, SEB, and Föreningssparbanken.
- **Credit and debit cards.**
  VISA and MasterCard.
- **Giro payment.**
  Postgiro and Bankgiro.

If the customer chooses to pay with a card, he or she first has fill out a form with his or her home address and then Goyada will send to their home a personal code, which binds the code-holder to the address specified. It takes a couple of days to receive the code and thus being able to refill the refill card is not immediate at all.

It is the same way with the giro payment method. When Goyada registers the payment, which takes up to six weekdays, Goyada sends a SMS to the customer containing the reload code.

7.2 Halebop

Halebop has lots of information services like weather, stocks and lottery reports. The customers can also compose their own ringing tones and draw their own operator logos. All services are totally free for the customer. Therefore Halebop does not need to have its own currency or loyalty point system. The result is that Halebop does not offer their costumers the ability to make real money payments, which results in that Halebop are not able to offer their customers the ability to purchase digital products like update codes for mobile phone refill cards. [107]

7.3 IOBox

The Iobox mobile portal includes much personalization such as favourite bookmarks, address book, and calendar. They are offering a few information related services. The ones they are offering are simple ones like news, weather, and lottery drawing reports. [108]

Iobox has its own portal currency, which they call credit. All their services cost a specific number of credits. The customer can refill their credit-account through the web, using any of the following payment methods:

- **Credit and debit cards.**
  VISA, EuroCard, MasterCard, and American Express.
- **Giro payment.**
  Bankgiro.

Iobox does not offer the consumers the ability to use their credits to purchase any digital goods. The credits can only be used for internally services in the portal like news, SMS, etc. Iobox does not offer their customers the ability to reload their mobile phone refill cards.

7.4 Room33

The Room33 is a combined Internet and mobile portal. They offer services like weather and stock information and also services like a calendar with reminders sent to the mobile phone in SMS format. Most services are just available for viewing on the Internet and are not sent to the cellular phone. [109]

All services in the portal are free and therefore Room33 does not need to have their own currency or loyalty-points system. The customer is not able to purchase any digital goods such as refill codes to their mobile phone refill cards because the portal does not have any payment solutions available.

8 Demand for Mobile Internet

This chapter tries to motivate why a start-up company like Celltribe acting in the mobile field should introduce some kind of own constructed cyber currency.

The motivation for starting acting in the mobile Internet field is crucial if one wants to investigate which payment opportunities one should offer the customers. The question is if it really exists a market out there that is willing to pay for mobile Internet services. If a company wants to provide services that are so good that people are willing to pay for them it is important to know what kind of value added services will be demanded. It is also important to start testing the market out already today to know what kind of services the market demands. Because this is such a fast changing market one needs to have the competence when the users request the service and not in sixth month after one discovers the demand. Then somebody else probably has done it already, therefore continues tests of the market must be performed.

Several m-commerce reports have been investigated in chapter 4. Some observations can clearly be drawn from them that motivate investment and speculation in the mobile Internet market.

One large piece of information that motivates that the mobile Internet demand will continue to rise is that the mobile penetration is predicted to rise in all European countries until 2003 when countries like Sweden and Finland, that already today have an extremely high mobile phone penetration, will come to a saturated level. Other less developed countries will with no doubt continue to follow Sweden's and Finland's example and continue to move towards the upper right corner in figure 8.1.

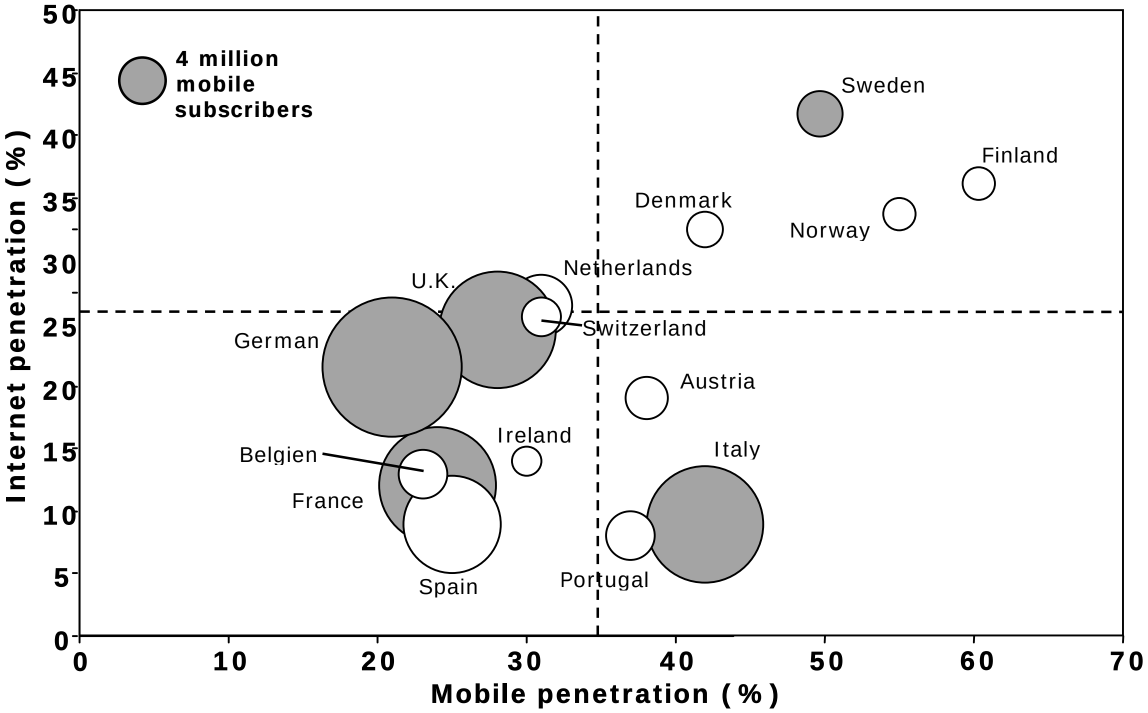


Figure 8.1. The current situation in Europe.[source: IDC]

Another motivation to start invest in the mobile fraction of the Internet is that the predictions show that before the end of 2002 the reach for mobile e-commerce will be greater than the fixed one. The distance between the two fractions is expected to grow larger and larger as time goes by, therefore the investments should be focussed on mobile commerce. Although the companies that are focusing on m-commerce most certainly must have great knowledge of the regular e-business parameters on the Internet, but they must also be aware of the fact that there are several parameter that are more important in the mobile case, logical navigation system and IO for example.

A large obstacle with mobile Internet today is the modest data rates that the current radio networks are able to offer the customers. This will partly be solved with the introduction of GPRS. It will take a considerable while until the technique finally penetrates the end user market, although GPRS already has been introduced in live scenarios for example in the United Kingdom, where it is not expected to reach a high penetration level, i.e. over 30 percent, until 2003. Extremely useful applications only available to the GPRS users might hasten the speed up. This is due to the fact that investigations show that people demand value added services and if these services only are available to the GPRS users the penetration of the technique would be faster.

Predictions also show that m-commerce revenues will change from that today mainly consist of providing information to by the year 2002 consist of a much wider spectrum of services like advertising, security, shopping, and entertainment.

A good way of testing what the market really wants is definitely to introduce some kind of system based on virtual cash or points.

8.1 CellPoint currency system

The CellPoint system can be categorized as a loyalty points system. It has the purpose of adding a feeling of importance of Celltribe’s services. By tipping friends and performing other tasks the user actually can earn CellPoints that can be used on offered value added services. As all other loyalty points system, it also has the purpose of getting more customers to the merchant. Introducing a loyalty points system is a cheap and rather straightforward way of spreading the trademark. It is extremely important that the services are that attractive that the customers will return.

8.1.1 Reason for CellPoints

In Celltribe’s case the loyalty points system in the start-up phase has the purpose of attracting new customers. By giving away loyalty points for tipping friends the company will increase the number of users in an easy way.

CellPoints can also be used to actually assign the services with a real value. In the first phase the value of a CellPoint in reality is nothing. No one would use the services if they would have to actually pay for it. Nevertheless the customer is aware that there exists some kind of point system. It is important to establish the concept from the beginning otherwise it would be hard to later introduce some kind of value system. Thus, it is better that from the start to make the users aware of the fact that even if the service in reality is not worth anything today it will in the future.

The addition of more services might justify an introduction of payments. The points system is also a flexible way of letting Celltribe choose the proper exchange rate.

Some new services might then be associated with a higher value than the services introduced in the start-up phase. The cost of the services can be regulated in an easy way. The actual “price” for all services should be kept at a low point level until a steady clientele has been established. Thereafter, when the customers have got used to the services as an everyday thing, the prices could be raised on popular and advanced services. The most important thing in the start-up phase is still to establish the concept amongst the users.

Another benefit with the points system in the Celltribe case is to increase revenues from advertising. The point system could be extended to reward users when for example visiting a banner. This could possibly increase advertising revenues.

8.1.2 Advantages compared to existing currencies

The advantage of having a loyalty points system in the start-up phase is obvious. The alternative of having a real payment system where the customers actually would pay for the services with an existing currency, i.e. SEK, is in reality not an alternative.

Each service would have such a low value that the standard payment methods like credit card and direct Internet banks absolutely are not alternatives. The consequence of this is that each user would have to have a prepaid account at Celltribe.

Since no micro payment systems have penetrated the market, there is no use in implementing one of them. Time will tell if for example Jalda becomes a success, in that case such a solution could replace the existing payment possibilities.

Therefore one clearly has to decide if each service should cost a certain amount of money or points. The alternative is that payments are done on a regular basis, for example a subscription based service. The subscription alternative could be designed so that for a monthly fee the customer is able to subscribe to a certain amount of service or as many services as desired. As long as there only exist SMS based services people will not subscribe to more than they actually want.

The subscription alternative with a monthly bill is nevertheless not in line with Celltribe’s business profile. No papers should be sent by regular mail, everything should be electronic. Therefore the best alternative is the credit card possibility, motivated in section 9.5. Although the credit card system forces the merchant to only accept rather large sums it is still the best alternative available today.

Therefore a solution where the services only cost points is suitable for the moment. This enables Celltribe to somehow implement a micro payment system, since a CellPoint can be worth only fractions of a Swedish crown.

Nevertheless the fact remains that the system must be designed in such a way that the user buys an amount of points. Different payment techniques have been presented and evaluated in section 9.1.

If using an existing cyber currency, like for example Beenz, Celltribe has no opportunity to control the exchange rate. Therefore, it is better to introduce ones own currency because it binds the user tighter to Celltribe. Beenz can be used on a lot of sites, but CellPoints can only be used at Celltribe’s own site. Therefore the customers are more closely connected to the company. The benefit of being exposed on the

Beenz site does not correspond to the cost of handling Beenz. Yet there exist very interesting opportunities, presented in the visionary section 8.1.3.

8.1.3 Vision

These loyalty systems offer a completely new opportunity. In a distant future it should be possible to use different types of loyalty points to pay for different types of services. A trading possibility should exist. It should be possible to exchange, for example, IKEA points and ICA points into Beenz as this then makes it possible for the user to purchase a certain service from an Internet site accepting Beenz as a valid currency. This would clearly add new value for all existing points systems. Small amounts of points from many different sources could then be exchanged into a large amount of for example IKEA points. This would add a great value for earning points from everywhere for everyone, since the user is able to exchange the “useless” small amount of points he earned at company A, B, and C to “useful” points at company X.

Implementing such an exchange system is not that difficult technically, but establishing legal contracts with all the participants could be harder. The exchange rate between different points system is also a matter of discussion.

9 Evaluation of existing payment methods

This chapter tries to motivate what kind of payment method or system is the best to use in Celltribe's specific case.

There exist several different techniques a merchant can implement letting the customer pay for his services. The available methods have been described in chapter 5.

9.1 Direct Internet payment

All large banks in Sweden are offering this service. The installation and integration processes are pretty straightforward. Either you must establish contracts with each and every bank or you can choose to use a third party as NetGiro or DebiTech. This is the leading payment possibility in Sweden today but it is only accessible from the web. However it provides the customer with a great amount of confidence. An interesting observation is that all direct Internet payment systems provided by the Swedish banks today is based on passing simple encrypted text string between the customer and the bank. None of them are using XML. The direct Internet payment service would be natural to implement for the Swedish market, but it is a unique solution for Scandinavia and it is not expected to spread to the rest of Europe.

For simplicity it is assumed that the four largest banks has approximately the same number of customers. As seen in figure 9.1 there are a rather large difference if one chooses to establish contracts with each separate bank compared to use a third party.

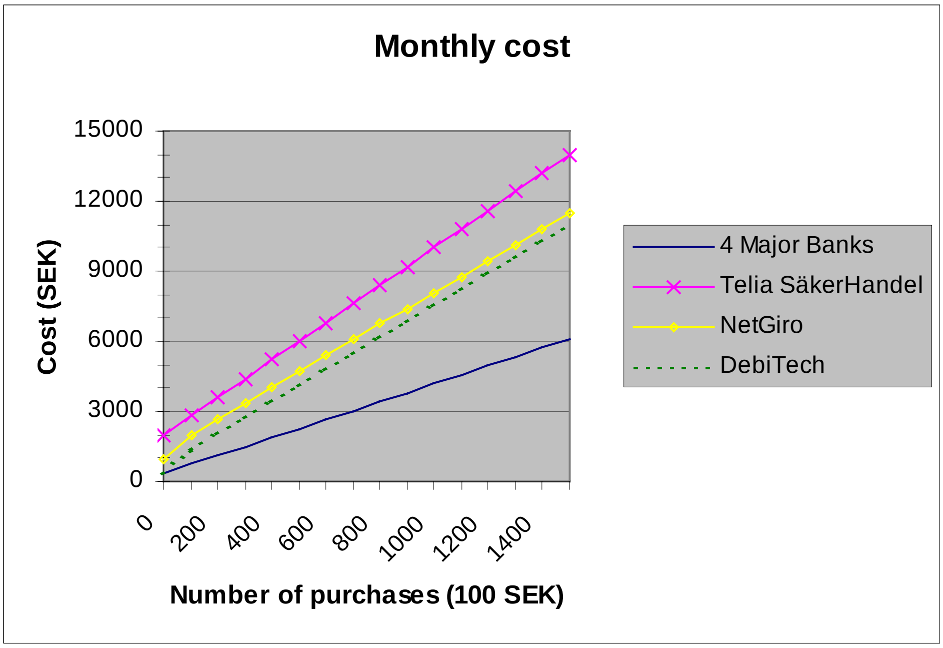


Figure 9.1. Comparison of the monthly cost of Direct Internet Payment.

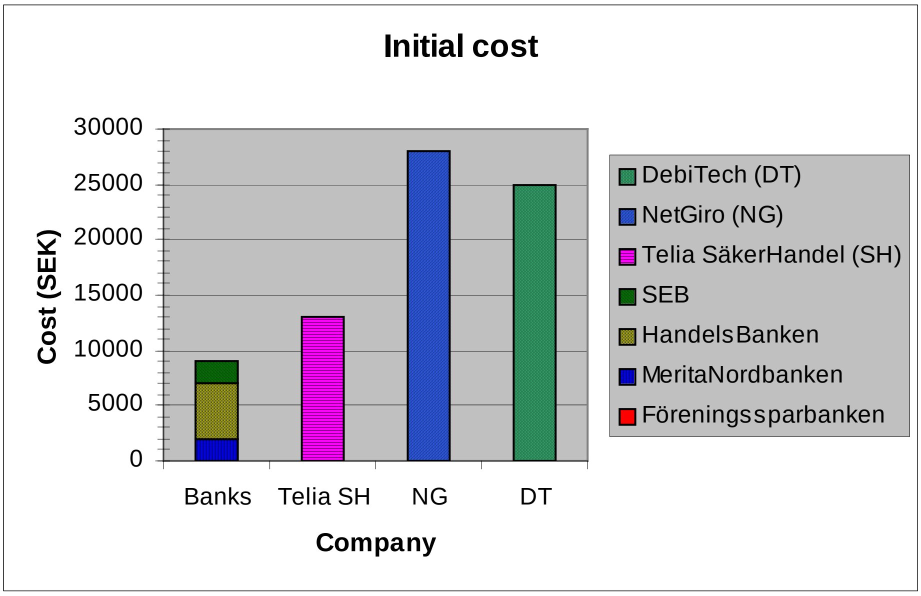


Figure 9.2. Comparison of initial start-up cost.

9.2 Credit Card

In the rest of the world, except in Scandinavia, this is the natural way of paying for merchandise purchased on the web. Therefore this payment method naturally should be possible to use in the web case. The credit card system does not care in what way the merchant gets hold of the credit card number. Therefore it can be retrieved through from practically every medium possible, SMS, WAP, CTI, or even voice.

In the credit card case it is always the company that takes the risk of losing money. If a customer uses a stolen credit card and the rightful owner reports that an incorrect transaction has been made, the bank will immediately refund the money to the customer from the company’s account, since the company has not been able to get a signature from the customer. This problem can be solved if the merchant chooses to implement the not so widely spread SET standard.

The advice to a start-up company is to focus on implementing a credit card payment system with for example the three largest card types, VISA, MasterCard, and American Express. For a pan European company American Express can be left out.

All Swedish banks demands that a SET engine is used when communicating with the bank. This is an expensive investment for a start-up company, which does not has a steady clientele. Therefore it is better to start with using a SET hotel like NetGiro or DebiTech. It is a rather modest cost for testing the demand from the market. If it turns out that the customers utilizes the service the company can later on choose to terminate the SET hotel contract and instead purchase its own SET engine.

In figure 9.3 Östgötabanken can be exchanged to any other of the large Swedish banks. The prices are almost the same. Östgötabanken is used as a reference since Celltribe is using their services today. The very high initial cost is due to the SET engine the company has to purchase if choosing not to use a third party.

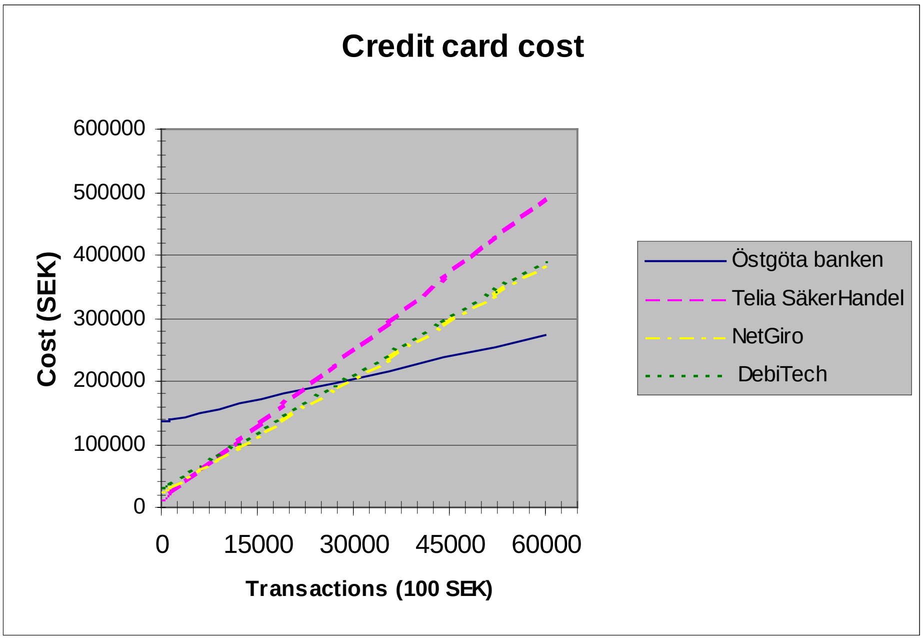


Figure 9.3. Comparison of credit card cost.

A start-up company like Celltribe is not expecting to perform a lot of transactions in the first phase. From the figure one can clearly see that the purchase of a SET engine is not motivated before you have performed nearly 30,000 transactions. Therefore a third party solution should be chosen. Telia SäkerHandel, NetGiro and DebiTech all can be said to offer basically the same services if one wants to add more services than the credit card solution in a later stage. As seen in the figure the alternative from Telia is much more expensive than the other two.

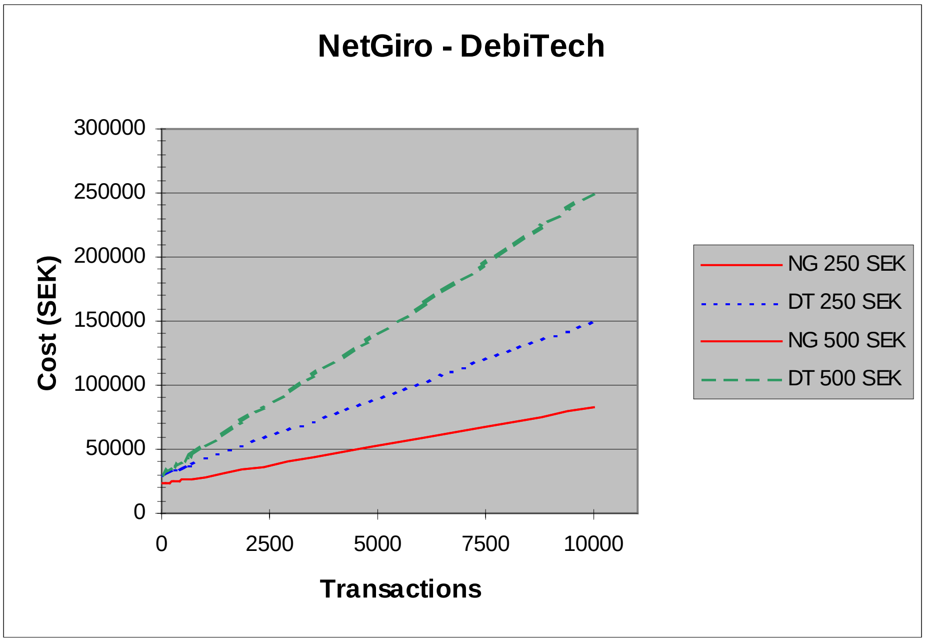


Figure 9.4. Comparison of credit card cost between NetGiro and DebiTech.

Since Netgiro has a fix cost per transaction and DebiTech uses a percentage cost it is more cost effective to choose NetgGiro as seen in the figure above.

9.3 Micropayments - Jalda

Micro payments can be expected to grow enormously in the future. However in the present moment most projects are in the trial stage. The most interesting alternative is Jalda that is backed up by large players like Ericsson and HP. The Jalda solution requires that the user has an account at an IPP and it will probably take a relatively long time before it penetrates the market. Also the Jalda API must be integrated in the system, which seems to be a lot of work if almost no one is able to use it anyway.

The fact that there does not exist a standard today indicates that start-up companies should not put a lot of money in a technique that they do not know will penetrate the market, however one should be aware of the fact that this is the next big thing. There is a huge possibility that the banks will take on the role to be IPPs since they already are used to handle transactions. Telia is about to establish itself as a Jalda IPP where users shall have the opportunity to refill their accounts using their phone bill or post/bank giro.

Jalda, or another micro payment system, will first be used on the Internet and it will probably take a while before it can emerge to the wireless medium. Probably GPRS is a condition for a successful wireless micropayment solution.

9.4 Special payment solutions

This section describes different alternatives that is available for use when implementing a payment structure for a website. Some can also be extended to the mobile medium.

9.4.1 Telia Säker Handel

This is a solution that offers the merchant to use practically every standard payment method available in Sweden today, such as direct Internet payment, credit card with or without special code, and invoicing.

An advantage with this solution is that only one contract needs to be written with Telia, not with every single bank. Also only Telia's system has to be implemented and not every single bank's. If one wants to have a solution with a lot of diferent payment alternatives up and running in a really short time Telia Säker Handel is definiatelly a good solution.

The price of this is not in porportion to what acctually is won. Especially the high transaction price, where almost half the fee goes to Telia.

9.4.2 Telia Advance 900

The main advantage with the Telia Advance solution is that Celltribe does not have to have any contact with another player, such as a bank or a SET hotel.

A huge disadvantage is that only wired phones connected to Telia's PSTN net can be used. The system is designed for listening on information, rather than payment procedures. Therefore the average transaction fee will be rather high. Also it is impossible to assign different fees to the same number so Celltribe would has to have multiple numbers if one wants to enable the users to purchase different amounts.

On the disadvantage list there is also the fact that Celltribe must deposit 30,000 SEK at Telia and have a quarterly turnover of 6,000 SEK.

9.4.3 Telia PayIT

Is available in two versions; eCharge and Jalda.

Version 1.0 eCharge
eCharge requires the user to have a modem and be connected to Telia's PSTN net. To the customer it becomes really complicated since the modem has to log off the current Internet connection and then re-connect to Telia's eCharge number. Consequently it is not expandeble to the mobile scenario.

A large advantage with this solution is that no vital information such as credit card number needs to be transferred. The user simply pays using his telephone bill and Telia transferes the money to Celltribe. Also the customer does not need to open a new account of any kind.

The disadvantages weights much heavier than the advantages, first of all is the modem technology old and for second it is not expandable to the mobile market.

Version 2.0 Jalda
The advantages and disadvantages with Jalda is described in section 9.3. Worth noticing is that Telia was running pilot tests in late September and is hoping to introduce the service in the beginning of November.

The advantages, as said before, is huge with a widespread micropayment system. The question is how long and exactly which solution that finally will penetrate the market. A start-up company should not bet on investing in Jalda today.

9.5 Conclusion

The best way for a start-up company to let its customers pay for merchandise must be to use either credit cards and/or direct Internet payment. A site focussing on the Swedish market should definitely implement direct Internet payment, since it has the higest user confidence.

For several reasons also a credit card alternative should be implemented. One reason is that this is the only alternative that today is possible to extend to the mobile market. In addition it is the standard way of paying on the Internet in the rest of the world. In Celltribe's case this means that a credit card solution could be used not only by the Swedish branch office but rather by the Spanish and German portals as well. Although a SET hotel should be used in the first phase since there will not be enough transactions to motivate the purchase of a SET engine.

Micropayment is definitely an opportunity that should be watched but until a high penetration of usage of for example Jalda is reached an investment is not motivated.

10 Potential mobile payment enabling technologies

This chapter briefly describes some different potential payment technologies, which can possible be used in the Celltribe case.

The security level of mobile solutions is of course extremely important when discussing using them for payment possibilities. This chapter describes the pros and cons with the techniques available today. There is a technology focus but this issue is also weighted with the purpose of a possible payment solution for Celltribe today. All conclusions should be seen in a start-up company’s view, where the company is only aiming for a small quantity of transaction of a restricted value.

The foundation of a mobile solution is often a working secure web solution. Running such service helps greatly for expanding a payment solution to the mobile environment. Therefore the web case is included as a reference.

10.1 Web

Using modern technology a very high security level can be achieved. Large companies, or in reality banks, can supply their customers with a separate smartcard or digipass that confirms the identity of the user. This solution is not applicable for a small start-up company.

All data sent over the Internet can be protected by IPSec or SSL. The standard algorithms used in those solutions, like SHA, 3DES, MD5, and RSA, can all be categorized as secure if used in a proper way.

10.2 SMS

The SMS technology is basically a small extension to the GSM standard. No extra security is possible to achieve, apart from the standard GSM 40 bits encryption. An SMS cannot be additionally encrypted since the standard does not support which algorithms that must be supported by the end device, i.e. the mobile phone. SMS decryption in the mobile phones would also require more computational and battery power to not deteriorate the performance level.

SMS is a non-session based form of communication. An authentication procedure is possible to achieve by combining both a short time code and a long time code.

Although the lack of possibilities SMS still must be considered to be an interesting technology if one wants to let the users initiate different orders from their mobile phones.

10.3 WAP

To be able to supply a complete WAP solution with end-to-end security the responsible system designer must guarantee security in two medias, both in the air (i.e. in the GSM net) and on the Internet. What makes this a complicated task is that these two medias communicates via two different protocol stacks. The WAP stack can be described as a slimmed-down version of the Internet stack, to compensate for the low transmission rate in the GSM net. The idea is very good, but the security has suffered from this slimming. In the WAP stack the equivalent to the SSL protocol used on the Internet is called WTLS. It is known to have several weaknesses compared with SSL (section 1.11).

Unlike transportation of data that is only using Internet as the transport medium it is theoretically impossible to keep the information encrypted and authenticated all the way from a user to an application server situated on the Internet. The security must be achieved in three different steps: between the mobile device and the gateway, in the gateway, and between the gateway and the application server. As the current WAP version and mobile devices are designed the information will never be secured all the way.

Over the air GSM supplies a 40 bits encryption that cannot be considered to be secure nowadays. Therefore the WTLS layer in WAP must be used to gain a higher security level. A problem with the WTLS layer is that it is used both to secure the data- and the transport layer, while the Internet usually uses IPSec to secure the IP layer and TLS to secure the transport layer.

Due to the fact that the WTLS session terminates in the gateway it is necessary to unpack the entire WAP stack all the way up to the application layer before a conversion to the Internet stack can be performed. This means that all information transferred using the WAP protocol can be seen in plain text in the gateway.

This problem can be eliminated if the company runs its own gateway directly connected with the application server, i.e. the Internet is never used as transport medium. An alternative is to only grant access to the application server to users that use some specific third party gateways hosted by certified and trusted parties. This clearly is not an acceptable technical solution but it might work with the right legal contracts.

The security between the gateway and the application server can be guaranteed by using standard SSL with 128 bit encryption.

The WAP solution can also be combined with other products like the E-mobilizer from WM-data and the SecureID from RSA (included in the R320 Ericsson mobile phone). The latter product functions much like a standard digipass, thus adding another level of security.

A solution to guarantee that the information sent cannot be seen in the gateway would be to actually encrypt the data higher up in the protocol stack, i.e. only encrypt the highest level. There exist a proposal for integrating and supporting a Wireless Identity Module (WIM) in the next generation of the WAP protocol. This hardware module would make it possible to place the encryption at the necessary level in the WAP stack.

10.4 SAT

SIM Application Toolkit, SAT (see section 6.5.3), is a standard that has co-existed with WAP and the latest standard phone models from the large manufacturers all support this standard. SAT is very suitable for a PKI solution, since a high security level can be achieved by storing the needed keys on the smart card. Several solutions have been developed using the SAT standard to achieve a proper level of security.

Nevertheless this solution is not possible for a start-up company to initiate. The initiative must come from other players like phone operators, etc. Nor does Celltribe have the competence to develop standard products and try to sell it to the large players in the market. Therefore SAT cannot be categorized as a viable alternative, for a small start-up company such as Celltribe that wants to implement a mobile payment solution.

10.5 CTI

Computer Telephony Integration, CTI (see section 6.4), is a concept that has been used for a long time by the Swedish banks. That means that the users feel confident using such services. In reality the security level must be considered to be low. This resembles from the fact that even if it is hard to overtake a session it is not that difficult to eavesdrop the DTMF tones sent over the telephone line.

However CTI must be categorized as a valid method for a small company to let its customers initiate mobile services including payment services.

10.6 Dedicated number

A dedicated number holds no extra security than the standard GSM encryption. The possibility of purchasing an exact number of points is limited by the fact that each value must have a unique phone number.

Moreover there is no authorization that it is the actual phone owner that is using the telephone. If someone can gain access to your mobile phone they are able to initiate just as many transactions as if you had lost your wallet. Since this system only depends on which phone that is calling a specific number.

Another negative issue with a dedicated number service is that it is only usable for the payment solution while the other alternatives such as a bonus can be used to let the user gain access to other services.

Because of the rather small adaptability and the limited user interaction the dedicated number alternative must be categorized as not interesting for a payment solution.

10.7 Conclusion

Thus, the three viable alternatives to introduce a mobile portal payment possibility are SMS, WAP, and CTI. How they could be implemented is further described in chapter 11.

11 Mobile payment solutions – a comparison

This chapter will describe and compare three different ways of mobile communication, which can be used for and implemented by a start-up company like Celltribe, to help them expand their payment possibilities to the mobile market.

The three medias are: SMS, WAP and CTI. The comparison will be based both on technology, security and business aspects. The way the user feels and the confidence he has got about the specific service is also taken into account. A large factor in the comparison between the different methods is what is right for Celltribe at the moment, both in the way of fitting into the current structure and what equipment is available.

11.1 SMS

SMS is an easy to use and easy to implement way to take wired transactions mobile. Although factors like the limited message length and the unfriendly text based user interface may outweigh the fact that almost every cellular phone is able to send SMS and therefore this method can be used by all cellular customers.

There are two different scenarios to conduct a transaction. First the scenario where the user takes the initiative and starts the transaction saying something like: “Buy 500 Points”. The second scenario is where the merchant takes the initiative and sends a query to the customer, asking if the customer wants to buy more Points. Such a query can be trigged and sent when the customer’s Point level falls below a certain value. In both cases the customer has to confirm the purchase by replying to the merchant’s message and for example including some kind of password. The merchant then has to send an acknowledgement of some kind to the customer containing the result of the purchase. That means that in the user initiated scenario there will be four SMS messages sent, two for the customer and two for the merchant. In the merchant initiated transaction there will be one transaction less for the customer.

11.1.1 Technology

Time to make a transaction
Depending on how many SMS messages that have to be sent between the merchant and the user, the total transaction time varies a lot. The average time for an SMS to reach the receiver after processing varies from 2-20 seconds. The large difference in time in Celltribe’s case is probably due to the fact that the SMS is sent through an independent SMS Central called Minick before reaching the specific operator. The differ in time can also be depending on which end-operator the SMS travels through and the priority it is given in each specific system.

Suppose that a complete transaction with acknowledgement requires 4 SMSs. That means that the user’s total inactivity time is somewhere between 8 and 80 seconds per transaction. The time it takes for the user to actively enter the requested data depends a lot upon the user. Let us approximate the user’s activity time for each SMS as roughly 45 seconds. In this case where the user has to send two SMSs. Additionally about 5 seconds computing time is added, this includes database lookups, clearing and debiting of credit cards, etc. If one assumes that the customer’s response time is 0 seconds the complete transaction will take between 103 and 175 seconds.

The most interesting part is nevertheless the time the user has to wait for a response from the merchant, the inactivity time. The inactivity time in the user initiating case is somewhere between 13 and 85 seconds and in the merchant initiating case somewhere between 11 an 65 seconds.

The times above are only an approximation and it is assumed that the SMS transmission takes the same time in both directions. More careful measurements are needed before an implementation should be done. Also the possibility of using GSM-modems to directly connect to each and every specific operator, without the need of going through a third party, must be considered. Although, that alternative will increase the cost.

Communication problems

There is no guarantee that an SMS ever reaches its addressee. If for example the user is temporarily out of range of the GSM network, the SMS will be queued at the operator and depending on when the user goes back online the SMS may or may not be delivered. Normally the operators keep undelivered SMSes for a couple of days before deleting them.

For some extra charge one can be notified by an SMS report, as to when an SMS reaches the receiver's cellular phone with a date and time stamp regarding a specific SMS message delivery.

Needed equipment and estimated cost

To be able to send and receive SMSs the customer only needs a regular cellular phone with the capability of handling SMS, which almost all phones are able to do. The merchant on the other hand either needs a network connection to a third party acting as an SMSC, where all outgoing SMSs are delivered to, or a GSM modem to directly connect to each operator who then delivers the SMSs. To be able to receive a message from the customer the merchant has to have a GSM modem.

The advantage of having the outgoing SMSs sent to a third party is that it is much faster to deliver it to the SMSC, and does not require establishing a GSM connection. Another advantage is that larger quantities can be delivered at the same time and at a cheaper cost. The price of a GSM-modem varies depending on vendor, but is somewhere around 3,500 to 5,000 SEK and has about the same capabilities as a regular cellular phone.

Cost for making a transaction (for Celltribe and the user)

The cost for the customer is the cost of one respectively two SMSs depending on which scenario is applicable. All operators have about the same price for sending SMS and it is about 1.5 SEK per SMS. The merchant cost is the same as the customer's if GSM modems are used for the outgoing traffic. If on the other hand the outgoing SMSs are sent through a third party SMSC the price is much lower depending on special agreements and large quantities.

Scalability

To be able to cope with an increasing amount of incoming SMSs investing in more GSM-modems is a simple solution. Another way of coping with an increasing amount of traffic is to lease a fixed connection to an SMSC. The outgoing messages are no direct problem. Large quantities enough are able to cope with the current Minick connection. There are no other known scalability problems regarding SMS.

11.1.2 Security

Encryption
A normal SMS has no special encryption except the standard encryption that the GSM net implements. Due to the fact that the SMS has a very limited message length of only 160 characters, adding extra encryption to the SMS could reduce the usable length of the message. Maybe a shorter message length is of no importance in this case, where the message just contains a few short words or numbers. The big question is in what way the cellular phones are able to encrypt and decrypt an SMS when they are not equipped with such a mechanism, at least not yet.

Authentication
To authenticate an SMS one would in the first step like to bind a certain SMS message to a specific GSM SIM card, i.e. a GSM phone number. The next step would be to bind the GSM number to a real person, which should result in that a specific person would be bound to a specific SMS and then the sent SMS would truly be authenticated.

Now, there are some factors that make it harder, or in some cases impossible, to bind a person to a sent message:

For instance the problem in binding a person to a specific number can be that the person is not registered with an operator. This is the case when the user buys his or her phone subscription as a prepaid account ('kontantkort' in Swedish) from a regular convenience store where no personal registration is needed. This means that there is no way one could trace a number to a real person.

There are also some problems or ways a person could use to avoid binding the GSM number to an SMS message. There is no problem when the person uses his or her cellular phone to send the message, because then the GSM number is always attached as a sender tag and thus bound. The problem comes if the user sends the SMS not from a phone connected to a SIM card, but from for example an SMS portal on the Internet or through an application program like ICQ. In most cases these portals and programs always attach their own sender tags, but if they would like to they could easily make it possible for the user to choose what should appear as the sender tag. One way to solve this is to always send some kind of confirmation or session code to the number specified in the sender tag and have the user reply with this code back to the company. This will at least bind that GSM number to the message.

User confidence
How the user feels about security when sending sensitive personal information like credit card number, personal codes etc is quite hard to measure. The overall impression is sending SMSs seems quite secure. The reason might be that there has not been that much said about it in media, as like for instance WAP or the regular Internet which people often say you should not send sensitive information over.

Involved medias
Normally, the complete transaction of SMS messages is carried out over the GSM network. Although the outgoing messages from the merchant can also be sent through a third party located on the Internet before being sent to each specific operator.

11.1.3 Business and User friendliness

Time-to-market
If after carrying out performance testing one chooses SMS to act as the user interface of the CellPoint mobile payment system, a complete implementation will take roughly about 2 weeks. Testing is not included in that time schedule.

Fitting the company profile
Using SMS as the user interface fits extremely well with the company profile, where almost all services are delivered to the customer via SMS.

User friendliness
To initiate and send an SMS with specific keywords that the user has to remember can be a pretty difficult thing to do. It is not comparable to a nice graphical web interface that points out exactly what data the user is supposed to enter. Most people are nevertheless familiar with sending and replying to SMSs, and there are many ways one can help to make the job easier for the user. For instance, the user should be able to enter abbreviations or even misspell the words and the merchant should anyway be able to interpret the phrase. If the user has entered totally incorrect data a syntax SMS can be sent to help the user enter the correct information. Also merchant initiated interactive conversations helps the user to know exactly what he or she is supposed to send back to the merchant.

Cost effective
No new equipment needs to be bought in at start-up. One can use the already existing SMS channels for the outgoing messages and GSM modems for the incoming ones. There is a transaction based cost though; the price of two SMSs, which varies depending on the current price using either the GSM modems or a third party.

Availability
The only thing the customer needs is a regular cellular phone, which can handle sending and receiving SMSs, which practically every current phone is capable of. Of course the customer also has to be in range of any operator's (for which their operator has a roaming agreement which includes SMS) GSM network.

11.1.4 Example service

In this section an example service is described. The specific service shown is when a mobile Celltribe-portal user wants to buy more CellPoints using SMS as the medium to communicate with the Celltribe portal system.

Flow chart
The figures below show the principles of how a payment service could be logically arranged. There are two different scenarios. The first described is when the user initiates the communication and the second is when the merchant somehow has decided that the customer might want to perform a purchase and in that case sends an initiating message to the customer.

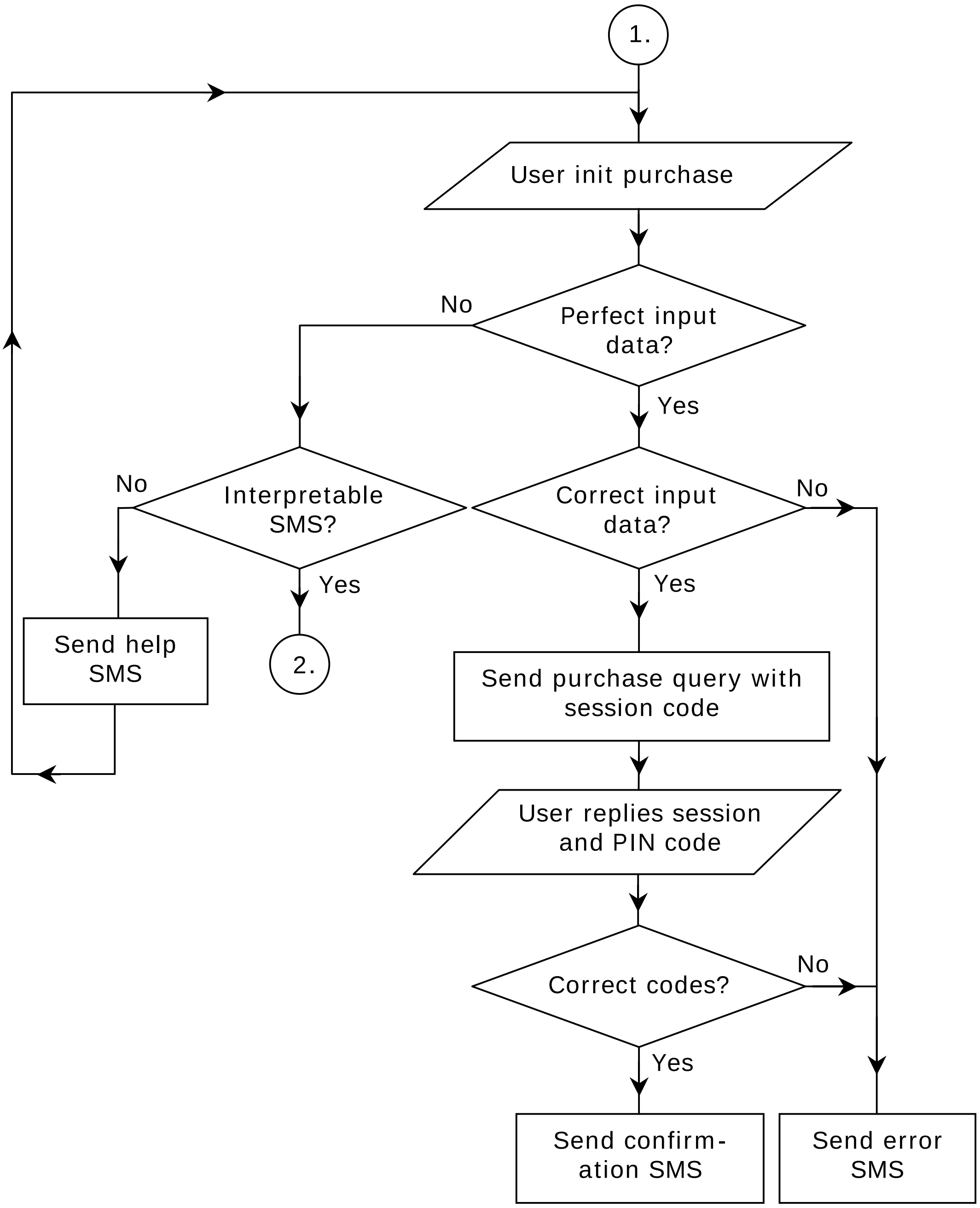


Chart 1: Shows the possible ways that the communication between the customer and the merchant can go, in the scenario where the customer initiates the purchase by sending a special phrase or words to the merchant. The phrase or words should somehow be understandable to the merchant in which case the merchant sends a session code, which the customer has to reply together with a PIN code to confirm the purchase.

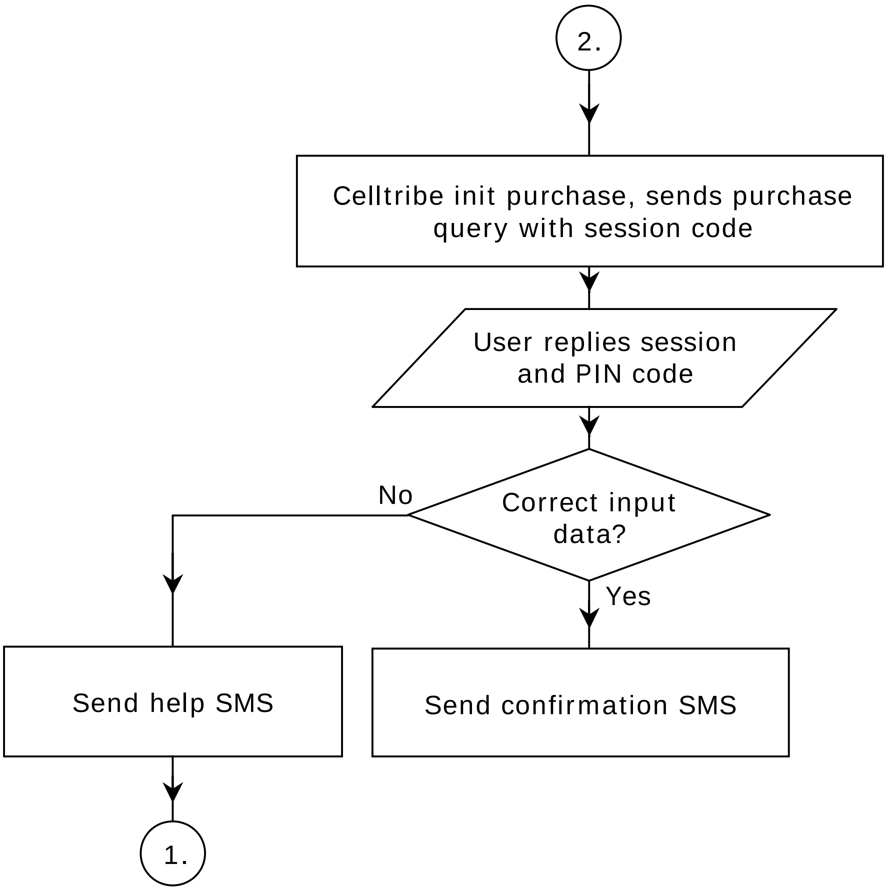
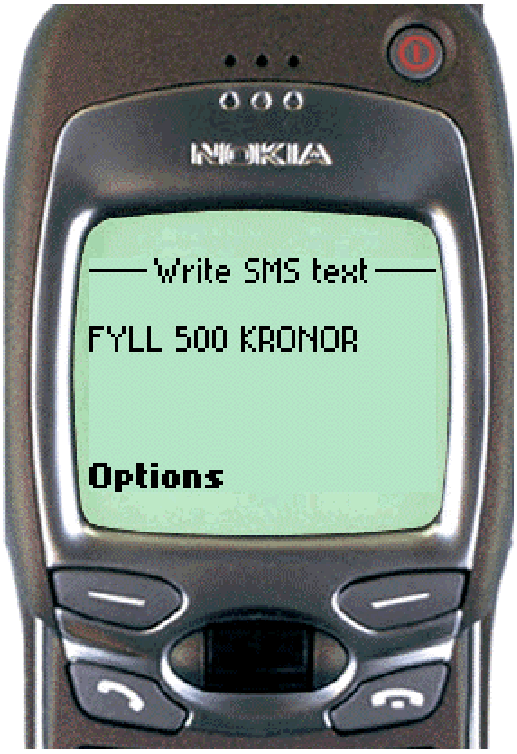

2.
Celltribe init purchase, sends purchase query with session code
User replies session and PIN code
Correct input data?
No
Yes
Send help SMS
Send confirmation SMS
1.

Chart 2: Shows the possible ways that the communication between the customer and the merchant can go, in the scenario where the merchant initiates the communication by sending a session code together with a request to the customer querying him to carry out a purchase. To commit to the purchase the customer has to reply to the query with the received session code together with his own PIN code.

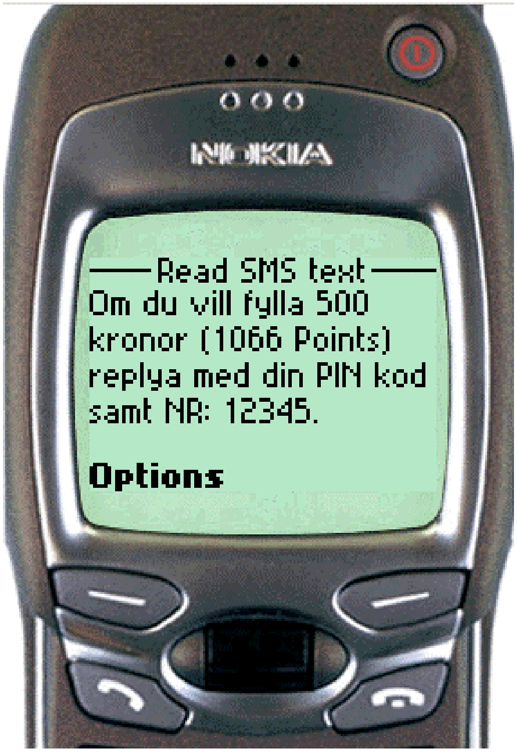
User interface
Below is an example on how it may look when a customer wants to buy CellPoints with a value of 500 SEK. In this case the user himself initiates the purchase by sending an SMS to the merchant. It is assumed that the user has preregistered his credit details.


Write SMS text

FYLL 500 KRONOR

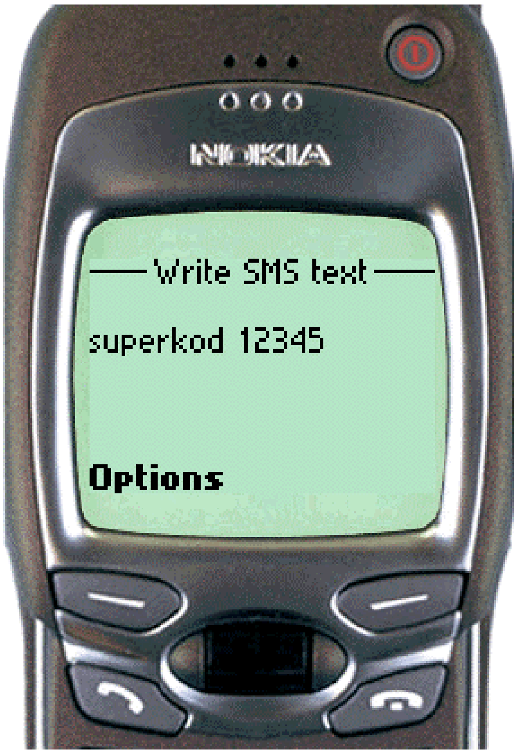
Options

Step 1: The user sends an SMS to the merchant with a phrase telling the server that the user wants to buy points to a value of 500 SEK.


Read SMS text
Om du vill fylla 500 kronor (1066 Points) replya med din PIN kod samt NR: 12345.

Options

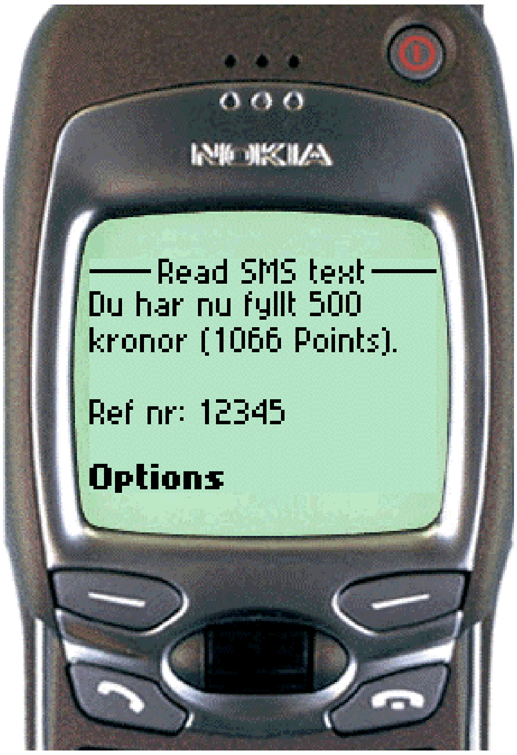
Step 2: The merchant replies to the user's SMS with a confirmation request and supplies a one-time-code.


Write SMS text

superkod 12345

Options

Step 3: The user confirms the purchase by replying his PIN and newly received one-time-code back to the merchant.


Read SMS text
Du har nu fyllt 500 kronor (1066 Points).

Ref nr: 12345

Options

Step 4: The merchant confirms that a purchase has taken place by sending receipt to the user containing a transaction reference number.

11.2 WAP

WAP is the data communication method that is spreading right now across the parts of the world that are using GSM. WAP enabled devices are being marketed by the mobile phone manufacturers and business reports says that WAP will penetrate the market in a near future especially with the introduction of GPRS. If a company today wants to develop a payment channel based on user interactive long-range data communication WAP definitely is an interesting alternative.

11.2.1 Technology

Time to make a transaction
The user needs to be online. Connecting to the Internet using WAP takes about 20 seconds. To navigate through the Celltribe deck with today's menu system would mean that the user would have to follow 3 links before arriving to the 'buy more points' section. We estimate this would take about 15 seconds. To navigate through these cards should be rather intuitive and the back-end system with database lookups, error checks, SET hotel communication etc. should not take more than a maximum of 3-5 seconds. With WAP the user can see exactly what he needs to enter in a form that resemblances the form used on the web. The input by the user, described in detail below, is estimated to take about 45 seconds. This results a total time of about 80 seconds but the time can be reduced to about 60 seconds if the user is already online.

Communication problems
The main problem is that the WAP server can be down or overloaded. In addition the data error rate is larger in a mobile network than in a fixed one, i.e. on the Internet.

Needed equipment and estimated cost
The customer only needs to have a WAP enabled mobile phone to take advantage of the WAP services Celltribe is offering.

What is needed for the merchant on the other hand depends on the desired security. If a WAP gateway is necessary the price depends on the manufacturer and the desired capacity. Melody Interactive offers a gateway that ranges from 8,800 SEK (3 licenses) to 200,000 SEK (100 licenses). Kipling offers their gateway for 50,000 SEK (5 licenses) and 500,000 SEK (100 licences). The alternatives from larger players like Nokia and Ericsson are even more expensive. Further evaluation of the different gateways should be done before choosing one. A WAP server is also needed to handle the incoming traffic.

Cost for making a transaction (for Celltribe and the user)
There is no cost for Celltribe after the initial start-up investments. However, the users need to pay a constant rate to their operator for the time they are online using Celltribe's services.

Scalability
It is comparable to the web case. Several WAP servers can run in parallel, it is the hardware capacity that limits the number of users. The WAP gateway can be upgraded with more licences as the number of users increases.

11.2.2 Security

Encryption
The WTLS protocol is used to secure the data from the handset to the WAP gateway. The WTLS session terminates in the gateway. If the gateway is situated at a third party IPSec or SSL can be used to secure the data sent over the Internet from the gateway to the end servers.

Authentication
Authentication is of great importance. When the user arrives at the WAP site Celltribe has no way of to knowing who it is that is using their services. Therefore a similar log in procedure as used on the web should be implemented. An alternative way would be to provide the user with a password when he opens an account at Celltribe. This password would bind the user to his credit card data stored in Celltribe's database.

User confidence
How the user feels about the security when sending sensitive information using WAP is quite hard to measure. Even though there has been a debate in the technical media about the security problems in WAP the user most likely feels that WAP is just as safe, or unsafe, as the Internet. An ordinary user is not aware of the gateway problem.

Involved medias
Once again it depends on where the WAP gateway is implemented. If Celltribe invests in a WAP gateway the traffic is passed directly between the GSM net and Celltribe's back end system. If a third party gateway is used the traffic will be passed over the Internet from that gateway to Celltribe.

11.2.3 Business and User friendliness

Time-to-market
A standard WAP service should be able to be implemented in about three weeks by binding it to the existing payment solution. The necessary WML programming is pretty simple. Nevertheless the limited IO opportunities means that the logistic aspects should be carefully considered before the implementation phase. Also the difference between different phone models will be a large problem. Investing in a WAP gateway must be evaluated and this will take a rather long time.

Fitting the company profile
WAP fits very well in Celltribe's profile, since the company aims to be a mobile content provider and WAP is the current data communication standard marketed by the large GSM phone manufacturers in Europe.

User friendliness
WAP is really slow to use. This will be improved by the introduction of GPRS. The interface and navigation system must be designed to be really intuitive. Nevertheless by using WAP the user can be guided to enter the right input to initiate a transaction much as on the web, but without all fancy graphics. A risk with investing in your own WAP gateway is that the user can only predefine five different gateways. Today a bookmark cannot be linked to a specific gateway. Therefore the user will have to manually choose to connect to Celltribe's gateway and that is certainly too much work for the ordinary user.

Cost effective
The only mayor cost for Celltribe is the initial investment. When the service is up and running only the standard transaction fee will remain. On top of this some operation costs will still be necessary.

Availability
To be able to use the WAP payment service the user needs to have access to a WAP enabled mobile phone. Also the customer's location must lie inside the coverage of a GSM network. Celltribe's obligations are to guarantee that the WAP server and WAP gateway is functioning properly 24 hours a day.

11.2.4 Example service

Flow chart
The figure below shows how a payment service could be logically arranged.

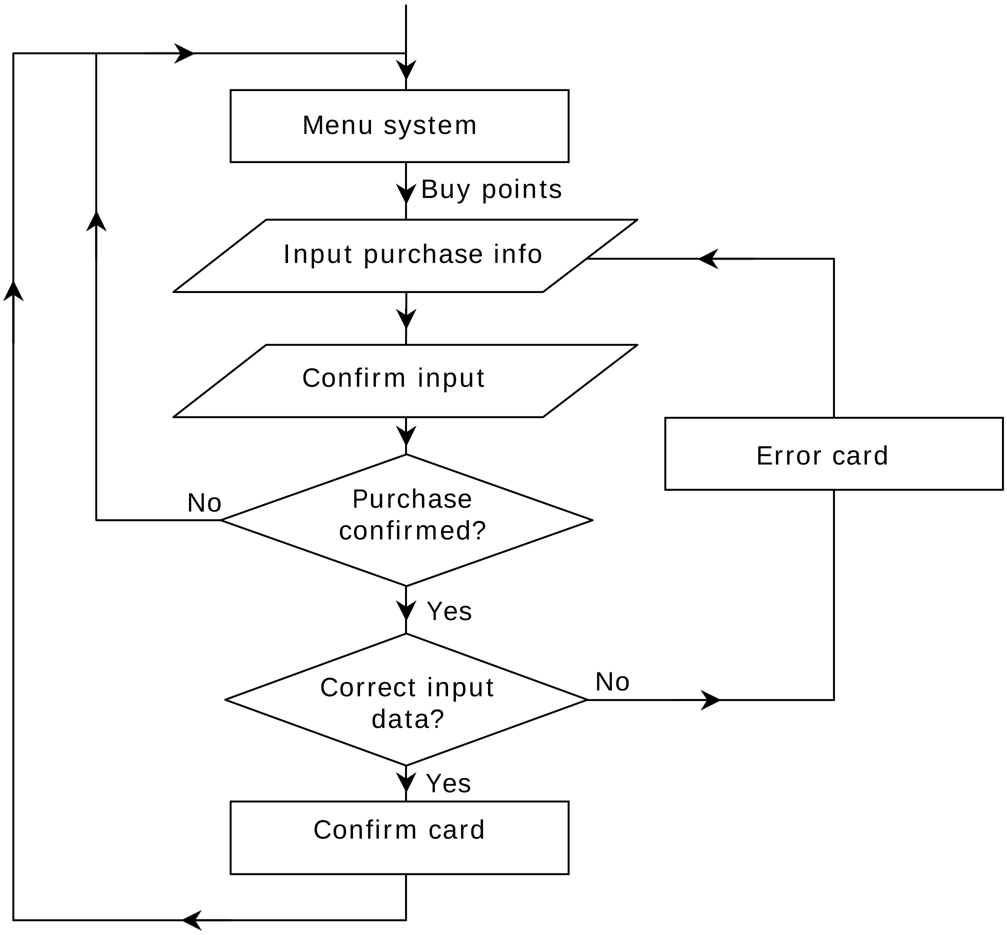
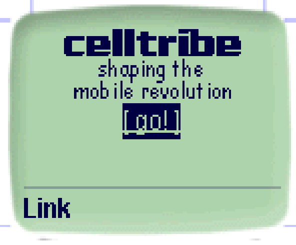


Chart 3: Shows the possible ways that the communication between the customer and the merchant can go. The customer logs in and browses to the correct WAP-page and then has to enter card information before committing the purchase.

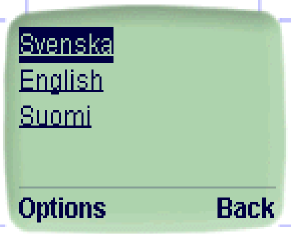
User interface

Below are some screenshots showing what it could look like when a user logs in on Celltribe's WAP site and chooses to buy CellPoints with his credit card. This demo was made with Nokia WAP Toolkit 2.0 with a WAP 1.2-enabled Blue Print phone.



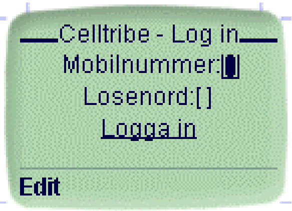
celltribe
shaping the
mobile revolution
[go!]
Link

Step 1: The user enters Celltribe's WAP site.



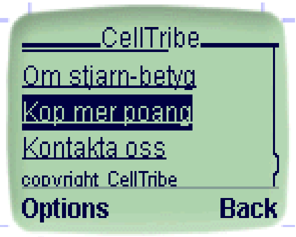
Svenska
English
Suomi
Options Back

Step 2: The user chooses to enter the Swedish part of the site.



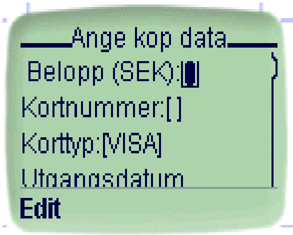
Celltribe - Log in
Mobilnummer:[]
Losenord:[]
Logga in
Edit

Step 3: The user logs in with his mobile phone number and a password.



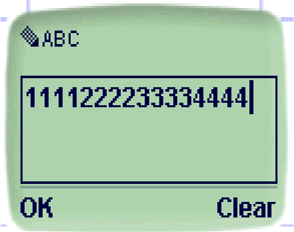
CellTribe
Om stjarn-betyg
Kop mer poang
Kontakta oss
copyright CellTribe
Options Back

Step 4: In the main menu the user chooses to buy more points.



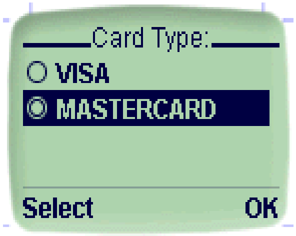
Ange kop data
Belopp (SEK):[]
Kortnummer:[]
Korttyp:[VISA]
Utgangsdatum
Edit

Step 5: A form is displayed and the user enters the required information.



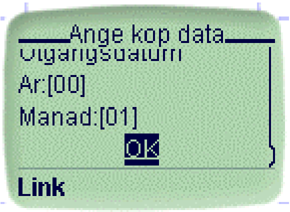
ABC
1111222233334444
OK Clear

Step 6: The user enters the credit card number in a text field.



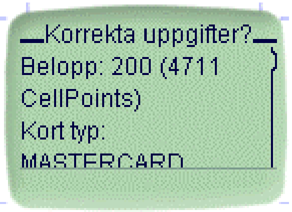
Card Type:
○ VISA
● MASTERCARD
Select OK

Step 7: The user enters the credit card type using radio buttons.



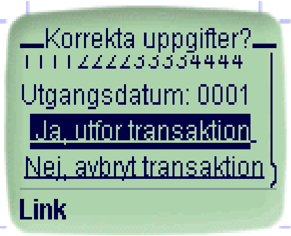
Ange kop data
Utgangsdatum
Ar:[00]
Manad:[01]
Ok
Link

Step 8: After entering all needed information the user presses OK.



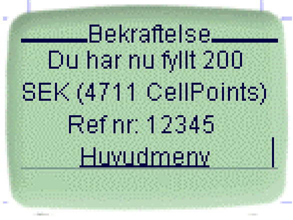
Korrekta uppgifter?
Belopp: 200 (4711 CellPoints)
Kort typ: MASTERCARD

Step 9: All entered information is displayed to the user. Including how many CellPoints he will buy.



Korrekta uppgifter?
1111222233334444
Utgangsdatum: 0001
Ja, utfor transaktion
Nej, avbryt transaktion
Link

Step 10: The user can choose to perform or abort the purchase.



Bekraftelse
Du har nu fyllt 200 SEK (4711 CellPoints)
Ref nr: 12345
Huvudmeny

Step 11: If the user chooses to buy CellPoints he gets a confirmation after the purchase has been done.

11.3 CTI

A classical communication channel between a merchant and a user is a touch-tone system. The user calls a number and is then transported through a voice messaging system by choosing different alternatives by pressing buttons on the phone. All interaction between the telephone system and the computer system is categorized as Computer Telephone Integration (CTI).

11.3.1 Technology

Time to make a transaction
There exist no bottlenecks in a CTI system. All operations are initiated immediately. Nevertheless the user has to navigate through the voice messaging system pressing the right buttons, thus the logistic design of the system is of great importance. The resemblance to the limited guidance opportunities with WAP is significant. The user would have to press an estimated 3 buttons before entering his personal information such as credit card information, telephone number, and PIN code. The entering of this information will probably take less time than in the WAP and SMS case and the user is never inactive waiting, either he listens to the messages or he is entering information.

Communication problems
Communication depends only on the quality of the telephone connection, fixed or mobile. In Europe there are no problems with this, problems might arise when calling from developing countries, like for example in Africa.

Needed equipment and estimated cost
Required equipment is a card inserted in an ordinary PC and a program that enables programming of the card. The main card manufacturer is Dialogic, who has about 60-70% of the market. Another large player is NMS. Both companies are selling both analogue and digital cards.

Analogue cards do not use any signalling. They can only receive the 16 DTMF tones of which normally 10 are used. In the analogue case the CTI card can be said to manually call the switchboard. The CTI server typically gets information about the A-number (source), B-number (destination), and C-number (if the call has been forwarded). All this information is transferred in serial communication, i.e. one digit after another. Every digit takes about 100-200 ms. There also exists a risk of noise interference if the CTI server is placed far from the switchboard. The cards can be purchased with different numbers of ports. The small cards have 4 to 16 ports. An estimated cost for a Dialogic card with 4 ports is 15,000 SEK and a card with 16 ports costs approximately 67,000 SEK.

Digital cards have access to all user information already in the alert phase (while the user is connecting) because it is sent via an ordinary packet net, typically using ISDN with 2 B channels and one D channel. An advantage with a digital card is that it is much faster than an analogue one. Furthermore the information is better protected against errors than in the analogue case. Using a digital card the CTI server is able to communicate with the switchboard during the whole “conversation”. With a digital card incoming calls can be put through faster. The price for a digital card is about 20 percent higher than the analogue one. For exempla Envox sells a digital Dialogic card called BRI2VFD for 1,900 USD (about 19,000 SEK) with four channels (2 BRI).

Each channel requires an additional license at a cost of about 300 USD. One can buy a rather powerful card but only start with a few licences and then add more channels by buying additional licences as the traffic increases.

The CTI cards can be programmed directly in C, but it is considered to be a rather difficult task, therefore there exist several CTI service design programs out on the market. Two programs with good reputation are Envox CT studio and Brooktrout ShowNTell. Both these programs have a graphical interface similar to other Windows programs. When buying the CTI card from Envox the software is included in the licence price.

The card prices above are for rather simple cards. If the company wants a more powerful solution improving the current switchboard functionality and advanced features like unified messaging then the prices lies in range from 150,000 to 200,000 SEK.

Cost for making a transaction (for Celltribe and the user)
After the initial software and hardware requirements have been made the service will not cost Celltribe anything. The user pays the standard telephone fee. An alternative would be that Celltribe assigns a 020-number to the CTI service and pays the user's phone cost. Another alternative is to get an 0771-number letting the customer call from anywhere only paying the local service fee.

Scalability
For a small to mid sized company a card with more capacity than needed at the moment can be purchased and only a few ports need to be opened. As the number of customers increases one can buy additional licences and open up these extra ports. It is worth mentioning that an ordinary server is capable of handling four cards with 60 ports each without any problems. In general there are no scalability problems in CTI solutions.

11.3.2 Security

Encryption
None. It is hard to take over a session but it is not that difficult to eavesdrop the DTMF tones sent over the telephone line.

Authentication
The CTI server receives the user's phone number if it is not protected, both when the user is using a GSM telephone or a wired one. These numbers cannot be faked, at least not in Sweden. In Celltribe's case the user would have to identify himself stating his mobile phone number. To actually make a transaction of any kind an additional PIN code would be needed.

User confidence
Although the communication can be eavesdropped relatively easy there is a great confidence in CTI services. This comes from the fact that the Swedish banks have been using these kinds of services for about 15 years.

Involved medias
If the user is calling from a fixed telephone only the Public Service Telephony Network (PSTN) is used. If the user is using a mobile phone both the GSM net and the PSTN net are used.

11.3.3 Business and User friendliness

Time-to-market
Choosing what kind of CTI card and program one shall use can be a complicated matter especially if the card should support more than simply a touch-tone system. The installation of a CTI card and a touch-tone system implementation are estimated to take about three weeks.

Fitting the company profile
CTI could make Celltribe's services available through the users' mobile phones, but it is not really in line with Celltribe's profile. Nevertheless it could be a complement to the other channels.

User friendliness
The interface and navigation system must be designed to be really intuitive. A smart navigation system is clearly a key factor to make any CTI service successful. A good design makes it easy for the user to fill in the needed data in a smooth way.

Cost effective
In general no cost except for the initial investments, if the company chooses not to have any special telephone number assigned to the service.

Availability
The user only needs to have access to either a mobile phone or a fixed telephone.

11.3.4 Example service

Flow chart
The figure below shows the principle of how a payment service could be logically arranged in a CTI environment.

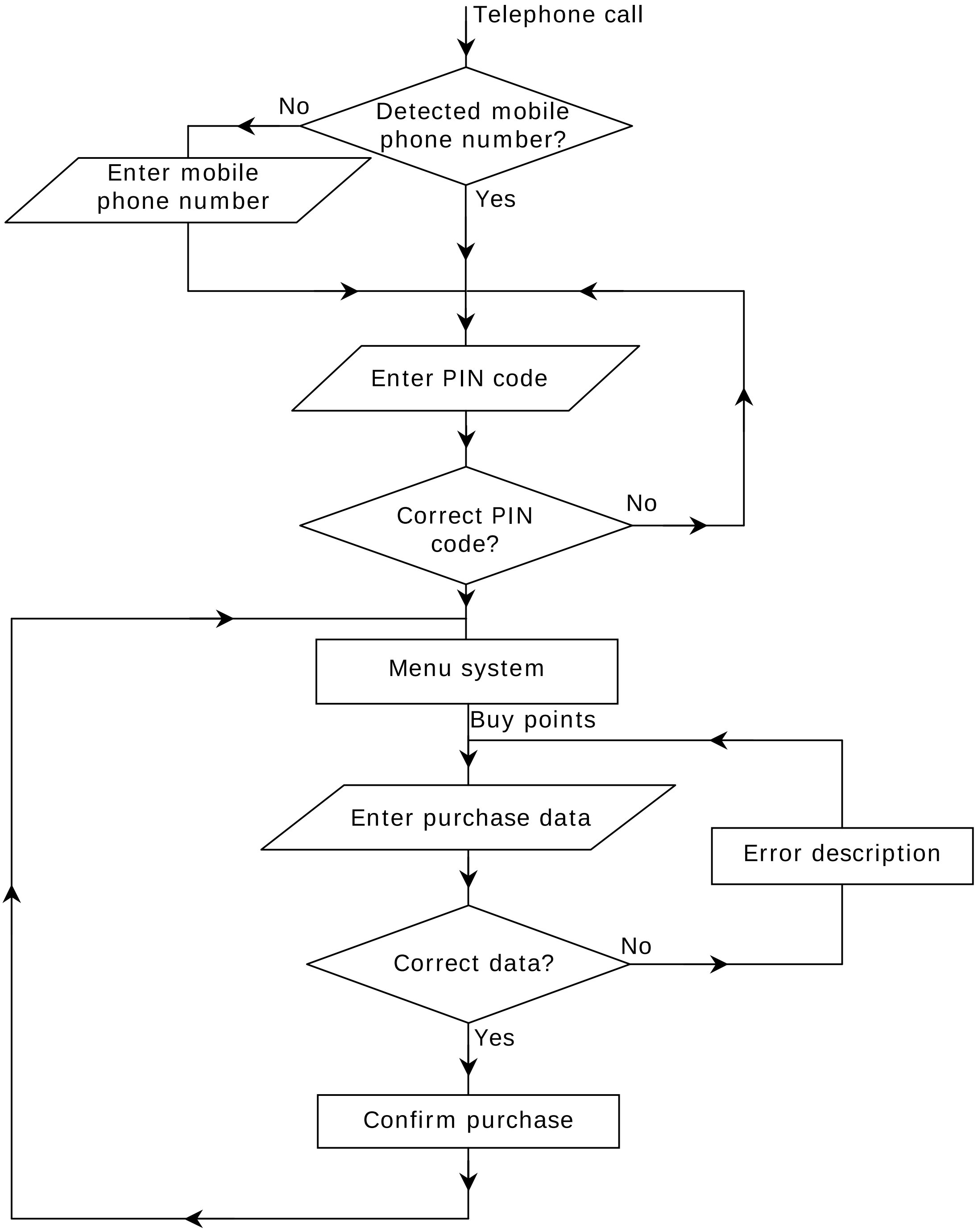


Chart 4: Shows the possible ways that the communication between the customer and the merchant can go. The customer makes a call to a dedicated number in the merchant's CTI system and depending on if he calls from his mobile phone or a phone connected to the PSTN he has to enter his mobile-number and a PIN code to authorize himself. A voice guides him through the menu system and the customer enters his credit details and purchase info by typing on his number-pad, which he also uses to commit the purchase.

How it works

The figure below shows how a CTI system could be integrated to the company's existing structure. The CTI card is placed in a NT machine and then connected to the existing switchboard. The NT's Ethernet interface is then connected to the company LAN, to make the computer able to do lookups in databases, execute external applications, etc.

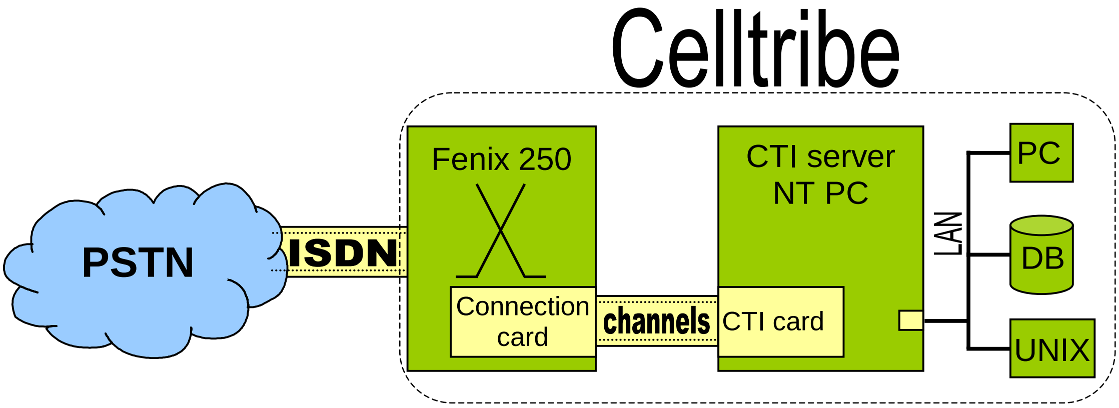


Figure 11.1. The general structure on how the CTI service is attached to the switchboard and the company LAN.

11.3.5 Calculation of needed lines

In a CTI system without any queuing possibility the main performance criteria is to determine the probability of blocking given an estimated stream of incoming calls, service time, and number of lines.

To motivate how many lines should be used when purchasing the CTI card these calculations have been done. The system can be categorized as an M/M/m/m system with Poisson arrival and exponential service time. The following data are estimated in the calculations.

Celltribe users, $C_u = 20{,}000$.
Estimated numbers of calls per month: 1 per user.
Average arrival rate, $\bar{x} = C_u / (3600 \cdot 24 \cdot 30) = 7.7 \cdot 10^{-3}$ s^{-1}.
Average service time, $\lambda = 120$ s.
Traffic intensity, $a = \lambda \cdot \bar{x} = 926 \cdot 10^{-3}$ Erlang.

With these parameters the well-known Erlang's loss formula can be used, *m* is the number of servers used, in this case ingoing lines.

$$B(a,m) = \frac{a^m / m!}{\sum_{k=0}^{m} a^k / k!}$$

Under these conditions the blocking probabilities listed in figure 11.2 can be calculated. As seen a good choice of ingoing lines is four, that since it means that only a little more than one percent of the customers will be blocked when calling the service. As seen in figure 11.2 there is no point in buying more than four licences.

Incoming lines	Blocking probability (%)
1	48.0800
2	18.2100
3	5.3200
4	1.2200
5	0.2200
6	0.0340
7	0.0046
8	0.0005

Figure 11.2. Different blocking probabilities.

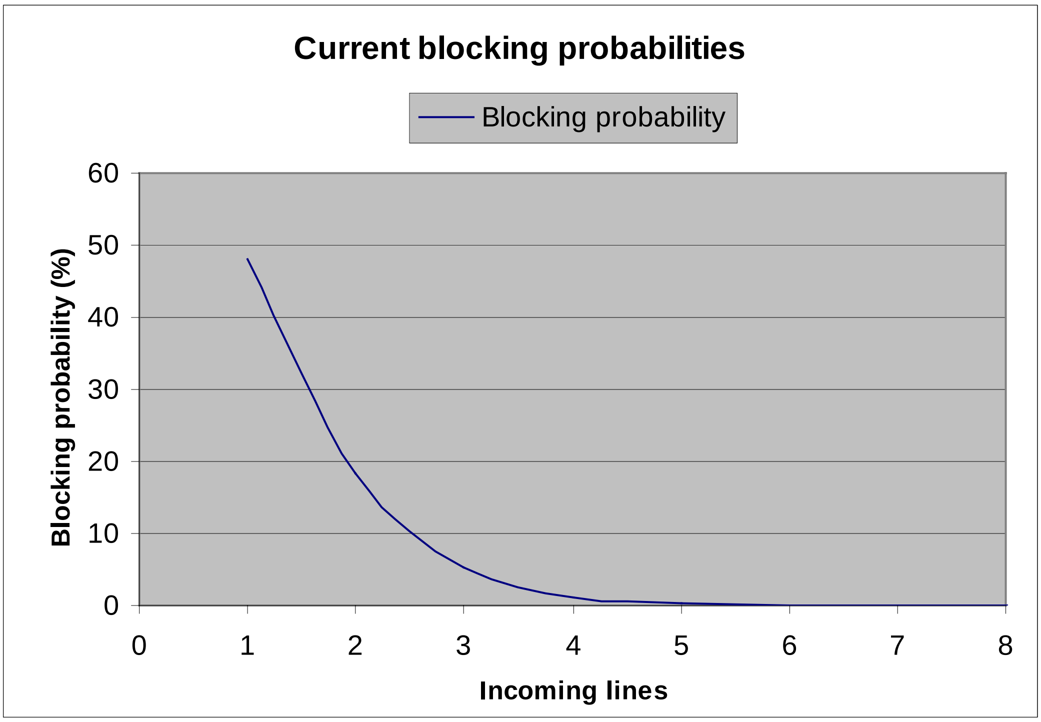


Figure 11.3. Start up phase description.

Even if the calculations above motivates a four channel CTI card the parameters could change rapidly. An example is shown below where an assumption is made that there exist many more Celltribe users. This means that the traffic intensity has risen from for example $926 \cdot 10^{-3}$ to 926 Erlang in the case that there exist 200,000 users. Given that all other parameters are unchanged the following table shows the blocking probability.

Incoming lines	Blocking probability, 200,000 users	Blocking probability, 100,000 users	Blocking probability, 50,000 users
4	62.29	36.7900	12.920000
6	45.25	16.3900	2.130000
8	30.24	5.3600	0.202000
10	18.01	1.2300	0.012000
12	9.22	0.2000	0.000490
14	3.92	0.0230	1.44E-09
16	1.35	0.0021	3.21E-11

Figure 11.4. Different blocking probabilities.

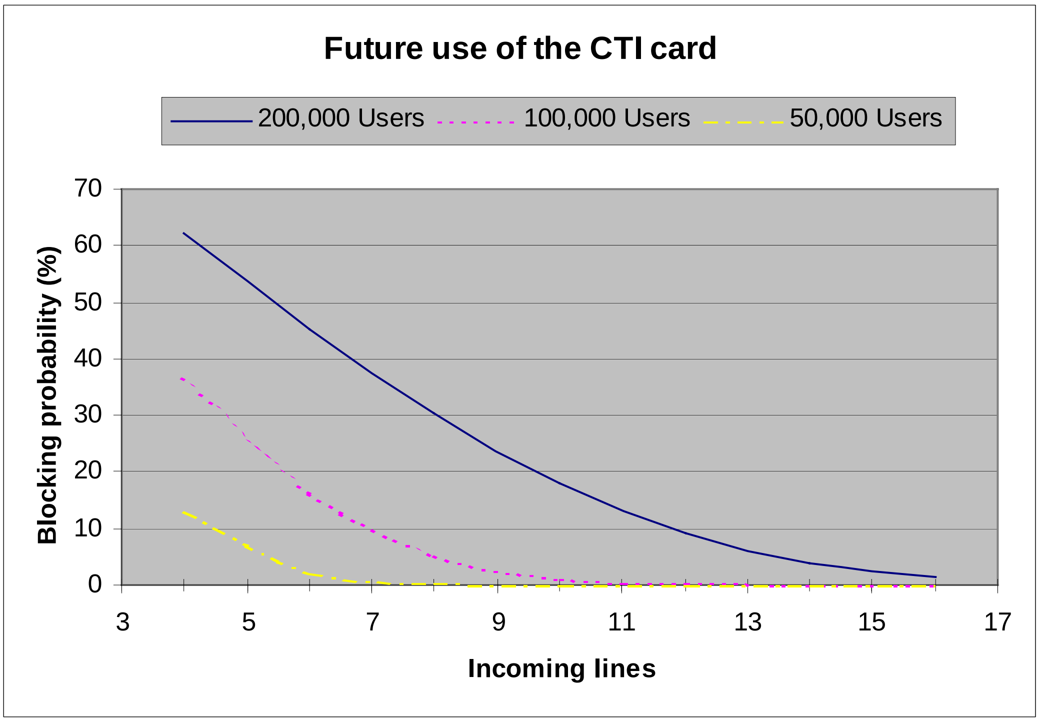


Figure 11.5. Possible future meaning that more licences need to be purchased

To further decrease these numbers a queuing system could be implemented in the switchboard. One should remember that the average calling frequency in the example above is rather low. If all portal services and questions should also be implemented in a CTI variant (opening up yet another channel for the users) the numbers will change.

	Web	SMS	WAP	CTI
Technology				
Transaction time (inactivity time).	3-5 seconds for debiting the card.	13-85 seconds for all four SMSs, including debiting the card.	3-5 seconds for debiting the card + about 20 seconds if a WAP connection has to be established.	3-5 seconds for debiting the card.
Communication problems	Web server down. Poor Internet connection.	No guarantee that an SMS reaches the destination.	WAP server down. Poor Internet or GSM connection.	None.
Equipment and cost (merchant)	Needs a web server.	Either just GSM-modems or GSM-modems for incoming messages and a third party for the outgoing ones.	Needs a WAP server.	Needs a CTI card in an NT machine and a special program communicating with the card.
Transaction cost (merchant)	None.	The cost of sending two SMSes.	None.	None, or maybe the cost of having a 020-nummer.
Scalability	Extremely good. There will be no great problem if the number of users starts to increase.	Good. If the number of users increases, more GSM-modems might be needed.	Extremely good. There will be no great problem if the number of users starts to increase.	Good. Depending on what card one invests in at start. One only need program licenses for the channels one uses.
Availability (customer)	Needs an Internet connected computer with a browser.	Needs a cellular phone and be in range of the GSM operator's net coverage.	Needs a WAP phone and be in range of the GSM operator's net coverage	Needs either to have a cellular phone with net coverage or a regular phone connected to the PSTN.
Security				
Encryption	SSL 128 bits.	Standard GSM.	In the air: Standard GSM (+WTLS). In the gateway: None. On the Internet: SSL.	None.
Authentication	Password, one-time-codes, smartcard + cardreader.	Password, replying of session codes sent to the mobile.	Password, one-time-codes.	Password, one-time-codes.
User confidence	OK. Frequent warnings of using credit cards on the net scares customers.	Good. There has not been that much said about SMS security in the media.	OK to Good. Media warnings scare costumers, but banks try to raise their confidence.	Very good. Banks and other institutions have used this alternative for years.
Involved medias	1) Just Internet. 2) Internet + modem (PSTN). 3) Internet + modem (GSM).	1) Just GSM. 2) GSM and Internet.	GSM + Internet.	1) Just PSTN. 2) Just GSM.
Business				
Time-to-market	Works already.	2 weeks.	3 weeks.	3 weeks.
Fitting company profile	Well.	Extremely well.	Well.	OK.
User friendliness	Extremely good.	OK.	Good.	Very good.

Matrix description of different issues, in the technology, security, and business area, of using SMS, WAP, and CTI to expand the payment possibilities on Celltribe's portal to the mobile market. The web is included as a reference.

11.4 Comparison

Below is a comparison of the three alternatives (SMS, WAP, and CTI) to expand the payment possibilities on Celltribe’s Internet portal to the mobile market.

11.4.1 Technology

Time to make a transaction is a key factor for which technique to choose. In this issue CTI holds a great advantage. Although WAP has a slow transmission rate the user is always aware that he or she is performing an action. SMS does not have a session system. Therefore the user is not aware of what is happening between the SMSs.

Some communication problems may arise. There is no guarantee that a sent SMS ever reaches its addressee. WAP and CTI are session-oriented services and if the user is able to connect to the service the user is most likely able to also finish the transaction.

The equipment needed varies and so does the cost. An SMS service requires GSM modems that Celltribe already owns. A WAP solution needs a WAP server to be up and running, Celltribe has got that. However, to set up an adequate security solution a WAP gateway is required. A CTI service requires a CTI card that is installed in a PC and connected to the switchboard. Generally speaking SMS is the cheapest solution to invest in.

An advantage for the CTI and WAP solutions is that there are no running costs for Celltribe. For SMS there is the cost of sending SMSs.

The scalability must be considered to be really good in all three solutions.

11.4.2 Security

None of the solutions can be considered to be totally secure. WAP has known security problems with the WTLS layer and the gateway. SMS has no extra security beyond the standard GSM security. CTI uses no encryption.

All solutions require secret codes that the user must remember. The WAP solution would be very similar to the web case. The CTI version could be similar to the WAP case, but with touch-tone system and interactive voice response (IVR) instead of menus. In the SMS case authentication could be achieved by introducing a session code to guarantee that the user is using a mobile phone and not an application. This would of course add extra complexity to the SMS solution.

CTI has the highest user confidence. As noted earlier, this is due to being an established technique that has been used by Swedish banks for a long time. With SMS the overall impression is that sending SMSs feels secure. WAP probably has least credibility of these three techniques.

11.4.3 Business and user friendliness

SMS, WAP and CTI all require about three weeks of implementation. CTI requires investment in a CTI card and a WAP solution might need a gateway. These investments will take additional time.

An important issue is if the proposed solution really fits the company profile. Since the distribution of Celltribe's services already today is utilizing SMS this is the alternative that best fits the company image. WAP also fits the company image rather well, since it is a very similar channel to the web. CTI is not really in line with Celltribe's profile, but it could make Celltribe's services available through the users' mobile phone.

Another key parameter is user friendliness. To initiate and send an SMS with specific keywords can be a tricky thing to do. On the other hand, SMS is an established technique that many people use every day. WAP is more comparable with the web, without all the fancy graphics. The design of the navigation system is of extreme importance. It is even more important when implementing an IVR system in a CTI solution. WAP must be said to be the most user friendly technique of the three, followed by CTI.

Only the SMS variant that has a transaction based cost, which varies depending on the current price using either the GSM modems or a third party. Both WAP and CTI are nearly free after the initial investments have been made.

Another important issue is how high the availability is. The optimal would be if the customer could use the service at any time, from anywhere using any device. CTI is the solution that best fits this wish. It is not bound to the mobile phone as SMS and WAP are. The SMS and WAP solutions of course also are limited by the coverage of the GSM network.

11.4.4 Conclusion

At this stage it would be convenient to start by implementing the SMS solution, because the SMS variant certainly fits the company's profile best and no initial equipment needs to be purchased. When comparing the investment costs the SMS service must be considered to have a much lower cost than the others even if it is the only service associated with a transaction based cost. This should be considered in the context that the additional SMSs sent from Celltribe (trying to initiate purchases) will be an extremely low percentage of the total SMSs already sent to the Celltribe members.

One drawback if using our solution with a session code is the complexity of the system. This is motivated by the fact that you already today can send SMS from applications like ICQ and the next logical step is to be able to redirect the answer not to your ICQ but to your mobile phone. By implementing a "session oriented" service that binds the user with his or her mobile phone two factor authentication is achieved.

If using a third party (in Celltribe's case Minick) confidential information like session codes of course should be encrypted when sent over the Internet. In theory this is true but in reality it might not be necessary. It is very unlikely that these session codes can cause Celltribe any damage, since they are only valid for a limited period of time. Nevertheless if one wants to secure the data sent to Minick they offer a 128 bits SSL encryption. The cost of this additional security is a set-up fee of 800 DM and a monthly fee of 250 DM.

Since Celltribe is focusing on the European market and the services presupposes that the user has an SMS enabled GSM phone the next logical step is to enable two-way communication via SMS. The SMS choice is also motivated by the fact that people already associate Celltribe with SMS services.

Nevertheless it is important to point out that all three alternatives would add a new channel for Celltribe’s customers to initiate not only a purchase, but to utilize Celltribe’s services. The WAP solution would be a mirror of the current web portal with simplified graphic design. The CTI solution with voice being the substitute for text could have the same structure as the WAP solution. The SMS solution could be extended to let the user request not only payment possibilities, but any service he wants at whatever moment he wants it.

Before implementing a CTI service further evaluations should be done about which specific CTI card to choose. Before choosing a WAP gateway evaluation and field tests should take place.

12 Implementation of payment solutions

This chapter describes two live and working implementations, which we have developed to enable Celltribe's portal customers to buy more CellPoints using their credit cards. The first implementation can be reached using regular Internet web pages. The second one is extended to the mobile phone, using a kind of interactive SMSs to handle the communication.

An implementation of a mobile payment system always relies on a secure connection between the bank and the company, i.e. Celltribe. This connection is often using the Internet as communication media.

In a payment system legal contracts have to be established both between Celltribe and NetGiro (the SET hotel) and between Celltribe and the bank. These contracts enable Celltribe to perform a credit card transaction from any medium such as the Internet or a mobile alternative. The connection between Celltribe and the bank will always be the same, independent of the media the credit card information is transmitted over.

Therefore a strategy evolved that the implementation project should be divided into two different phases. The first implementation phase had the objective of enabling the company's customers to use their credit cards on the web portal. This implementation became a real product and it is described in section 12.1. The second phase had the purpose to extend this Internet based solution to the mobile market. After investigations of different technologies SMS was chosen and a demo product was implemented as described in section 12.2.

To increase the user confidence a 128 bit SSL has been installed on Celltribe's Apache web server. Therefore a re-configuration of Celltribe's Apache web server was needed to enable it to perform the transactions via a SSL protected mode, adding the proper new servlet zones.

12.1 User Interface – Web

This section describes how the credit card payment possibility can be implemented on Celltribe's portal. The system architecture is described and necessary components are listed. A user interface has been implemented and the design and functionality are described.

12.1.1 Description

This product includes three parts:

- Netgiro programs: Transaction classes, Merchant Server and CeloCom encryption server.
- An API, which consists of functions to charge credit cards using the Netgiro payment hotel. And also functions for logging these transactions in a database.
- A working demo/product was implemented in the Celltribe Mobile Services (CMS) Portal using regular JSP pages.

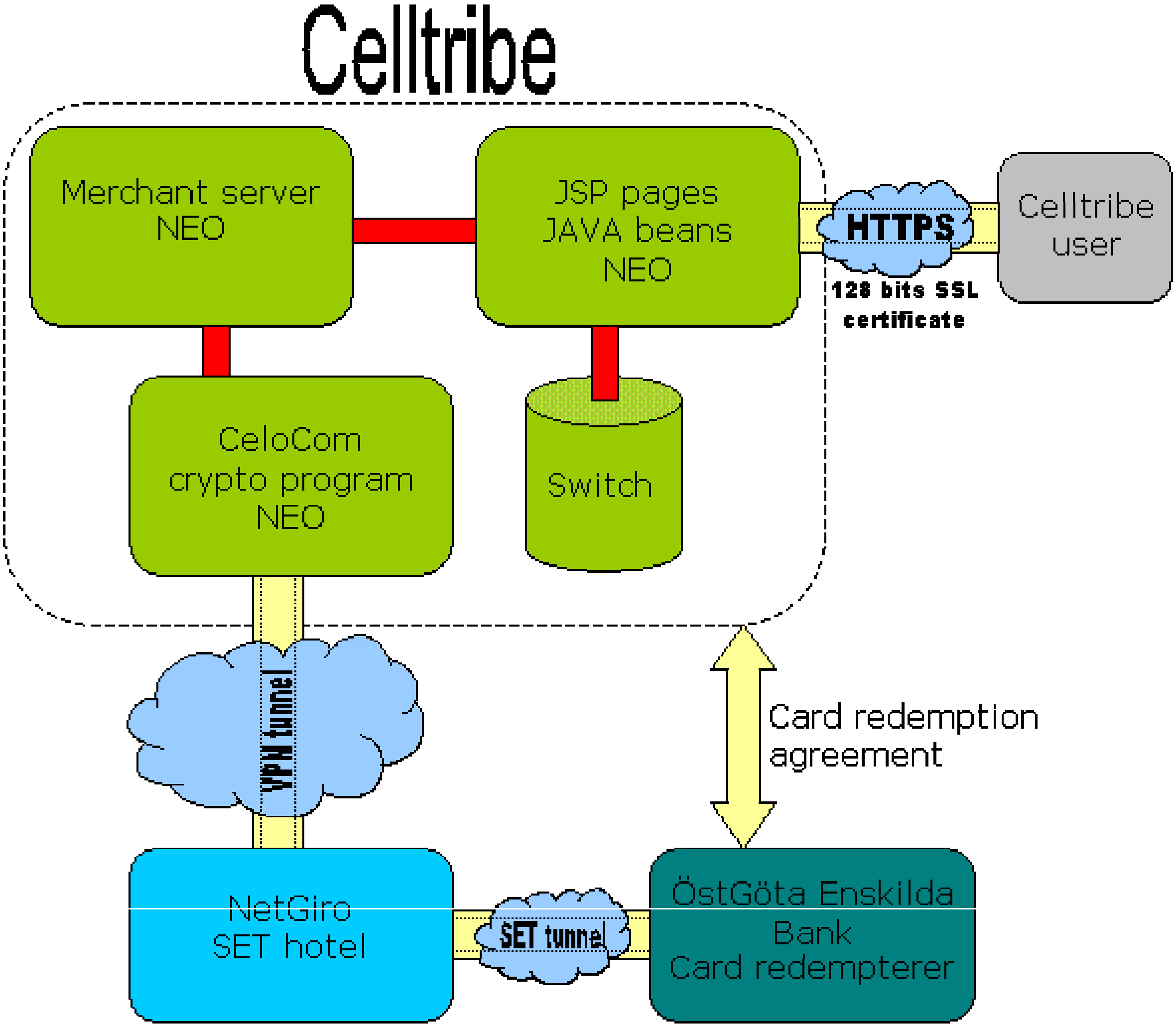


Figure 12.1. Schematic description of the web payment implementation.

12.1.2 Netgiro programs

The transaction classes are distributed in a file called `ClientAPI_211.jar`.

The MerchantServer is a Java program included in the jar file above. It handles the communication with the Netgiro server. It must be executed as root at the intended server. There is a `MerchantServer.properties` file connected to the MerchantServer, where information such as server ip, port, paths, etc. can be set.

The CeloCom encryption program is responsible for the encryption of traffic between Celltribe and Netgiro. The program is dependant on the configuration file `ssr.rc.` This file must contain exactly the correct information. Information such as ports and IP addresses must be the same as in `MerchantServer.properties`.

12.1.3 Java API

The Java API consists of the following classes in a package called `ppp` (Portal Payment Possibilities):

- ppp/pppConstants
- ppp/Payment
- ppp/NetgiroPayment
- ppp/NetgiroCard

pppConstants
This class is just a simple interface containing static constants like paths, names of databases, locations of servers, ports to use, etc. It is not the same information as in the MerchantServer properties file mentioned above, and the values are default values, which our other classes use.

Payment
Contains functions for querying and updating databases, handling logging of transactions, creating payment accounts, handling error messages and updates user information.

NetgiroPayment
Contains Netgiro related functions. Makes the connection to the MerchantServer and also creats the transaction object to be sent to Netgiro through the MerchantServer. It handles the transaction type DirectDebit, which validates the card and transfers the funds to the merchant's target account.

NetgiroCard
It is a GUI application to manually debit or credit an account. It handles the transaction type DirectDebit and DirectCredit, which transfer funds to the merchant's respectively customer's account.

The purpose of this application is just to be able to manually debit or credit an account. The later can be useful if for some reason the purchase needs to be undone.

12.1.4 Working demo/product

It consist of the following files excluding them above:

- `pay_credit1.jsp`
- `pay_credit2.jsp`
- `pay_success.jsp`
- `pay_error.jsp`
- `pay_err.jsp`
- `pay_account.jsp`
- `pay_agreement.jsp`

SSL should be used to encrypt the communication between the user and Celltribe. This is because both Celltribe and the user do not want credit card details to be sniffed from the net.

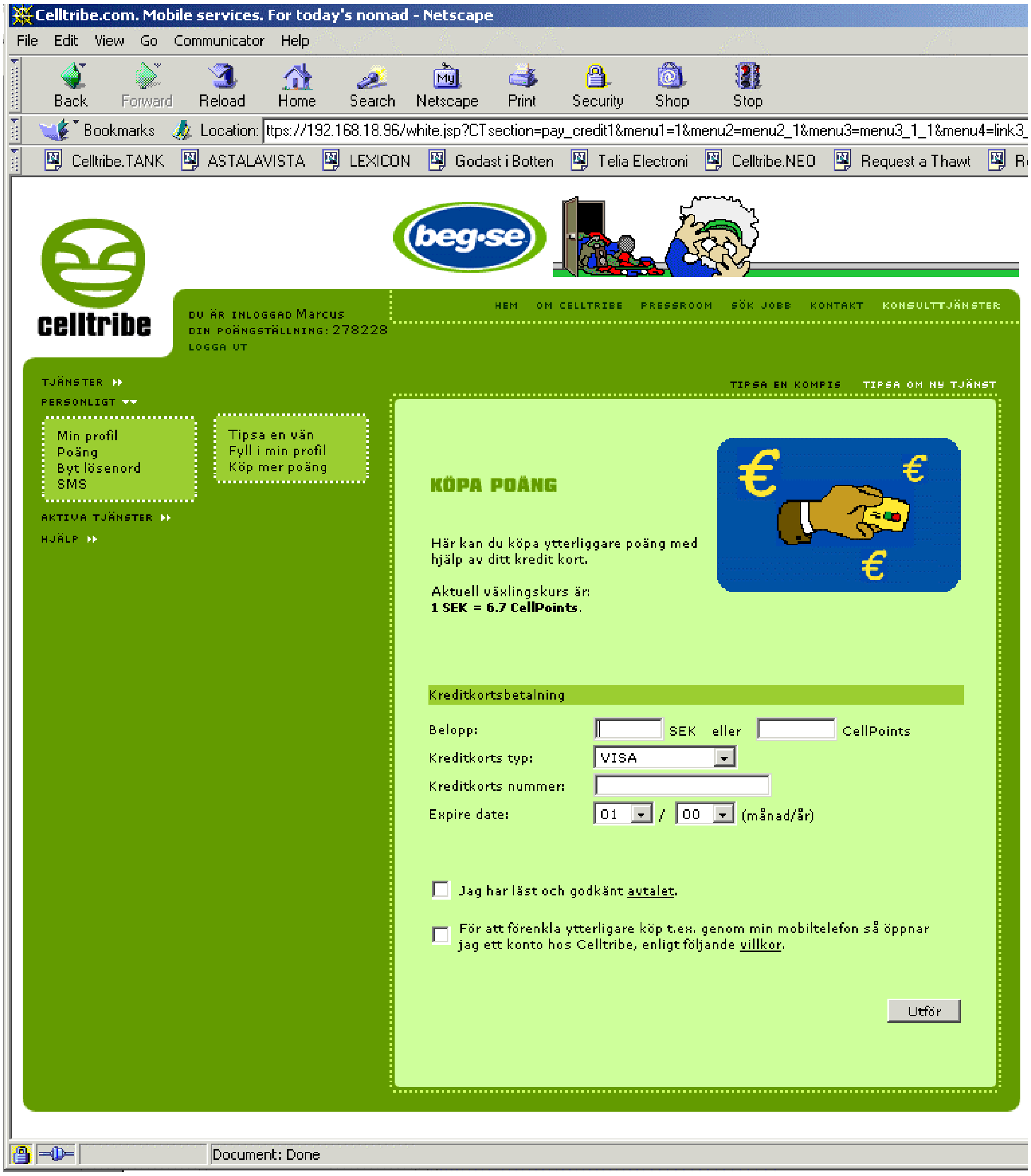
pay_credit1.jsp
This is the page the user first sees when clicking into the service. It consists of forms for entering payment data like credit card number, expire date, amount, etc. It also shows the current money-to-point rate. There are also two checkboxes, which are linked to different agreements. The first checkbox is mandatory and consist of an

agreement that the user must accept saying that the purchase is legitimate, and that the user is the rightful cardholder, etc. The second checkbox is optional, and if the user checks it, he or she agrees that Celltribe stores the credit card number and expiration date to make further purchases easier (for instance purchases from media other than the web, like SMS, CTI, WAP etc).

The user is able to specify the desired amount in either SEK or CellPoints. The amount with current rate is displayed in both the form-windows using javascript via a database lookup.

Each time a user enters the page a database lookup is made to check if the user in a previous session had checked the later checkbox. If that is the case, the credit card data is automatically inserted into the displayed form.

When the user has entered all data and hits the submit button, a javascript starts and displays a confirm window to the user. When the user confirms his/her order and waits for the reply (this takes about 3-5 seconds for a successful transaction and less for an unsuccessful one) the submit button is locked to prevent to user from hitting it again, which could result in multiples unwanted transactions.



Celltribe.com. Mobile services. For today's nomad - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location:
Celltribe.TANK ASTALAVISTA LEXICON Godast i Botten Telia Electroni Celltribe.NEO Request a Thawt
celltribe
beg·se
HEM OM CELLTRIBE PRESSROOM SÖK JOBB KONTAKT KONSULTTJÄNSTER
TJÄNSTER
PERSONLIGT
Min profil
Poäng
Byt lösenord
SMS
Tipsa en vän
Fyll i min profil
Köp mer poäng
AKTIVA TJÄNSTER
HJÄLP
TIPSA EN KOMPIS TIPSA OM NY TJÄNST
Utför
Document: Done

Location: ttps://192.168.18.96/white.jsp?CTsection=pay_credit1&menu1=1&menu2=menu2_1&menu3=menu3_1_1&menu4=link3_

DU ÄR INLOGGAD Marcus
DIN POÄNGSTÄLLNING: 278228
LOGGA UT

KÖPA POÄNG

Här kan du köpa ytterliggare poäng med hjälp av ditt kredit kort.

Aktuell växlingskurs är:
1 SEK = 6.7 CellPoints.

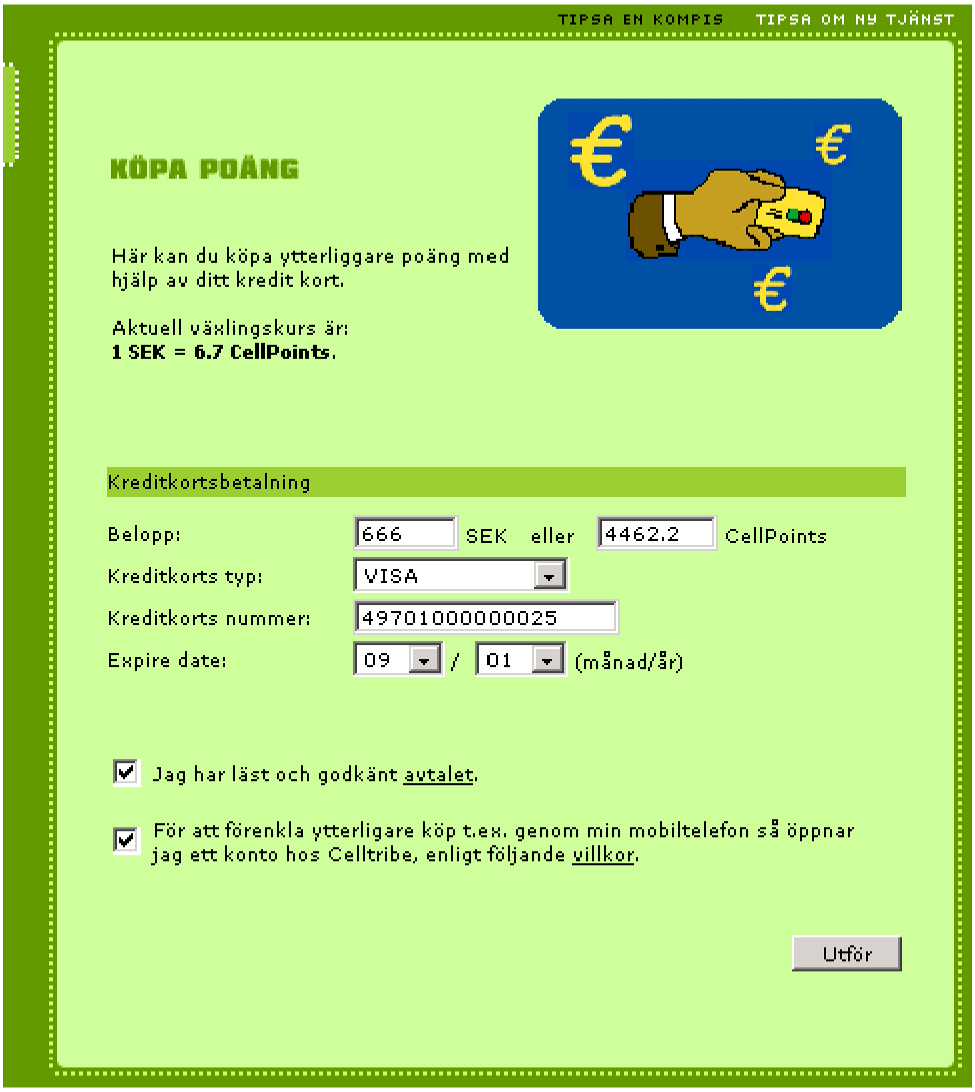
Kreditkortsbetalning

Belopp: [ ] SEK eller [ ] CellPoints
Kreditkorts typ: VISA
Kreditkorts nummer: [ ]
Expire date: 01 / 00 (månad/år)

□ Jag har läst och godkänt avtalet.

□ För att förenkla ytterligare köp t.ex. genom min mobiltelefon så öppnar jag ett konto hos Celltribe, enligt följande villkor.

Figure 12.2. This is how it looks in the portal.



KÖPA POÄNG

Här kan du köpa ytterligare poäng med hjälp av ditt kredit kort.

Aktuell växlingskurs är:
1 SEK = 6.7 CellPoints.

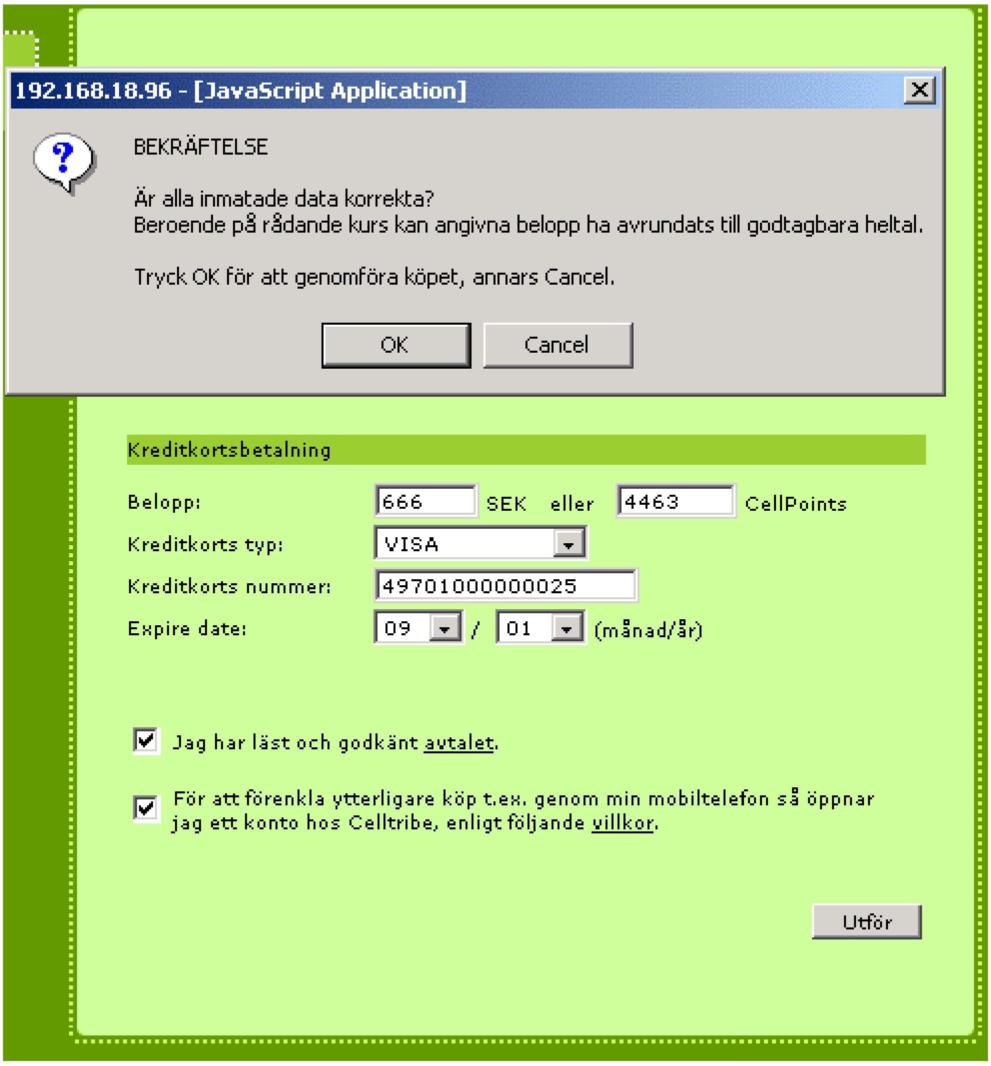
Kreditkortsbetalning

Belopp:	666	SEK eller	4462.2	CellPoints
Kreditkorts typ:	VISA			
Kreditkorts nummer:	49701000000025			
Expire date:	09 / 01 (månad/år)			

☑ Jag har läst och godkänt avtalet.

☑ För att förenkla ytterligare köp t.ex. genom min mobiltelefon så öppnar jag ett konto hos Celltribe, enligt följande villkor.

Figure 12.3. Step1: Fill in the necessary information. Here, even the optional last checkbox is marked.



192.168.18.96 - [JavaScript Application]

BEKRÄFTELSE

Är alla inmatade data korrekta?
Beroende på rådande kurs kan angivna belopp ha avrundats till godtagbara heltal.

Tryck OK för att genomföra köpet, annars Cancel.

Kreditkortsbetalning

Belopp:	666 SEK eller 4463 CellPoints
Kreditkorts typ:	VISA
Kreditkorts nummer:	4970100000025
Expire date:	09 / 01 (månad/år)

☑ Jag har läst och godkänt avtalet.

☑ För att förenkla ytterligare köp t.ex. genom min mobiltelefon så öppnar jag ett konto hos Celltribe, enligt följande villkor.

Figure 12.4. Step 2: When the user hits the submit button a confirm windows is displayed. The amount in the form is rounded. Compare with step 1.

pay_credit2.jsp

After the user has confirmed the transaction the pay_credit1.jsp file makes a GET request to the second JSP file (pay_credit2.jsp).

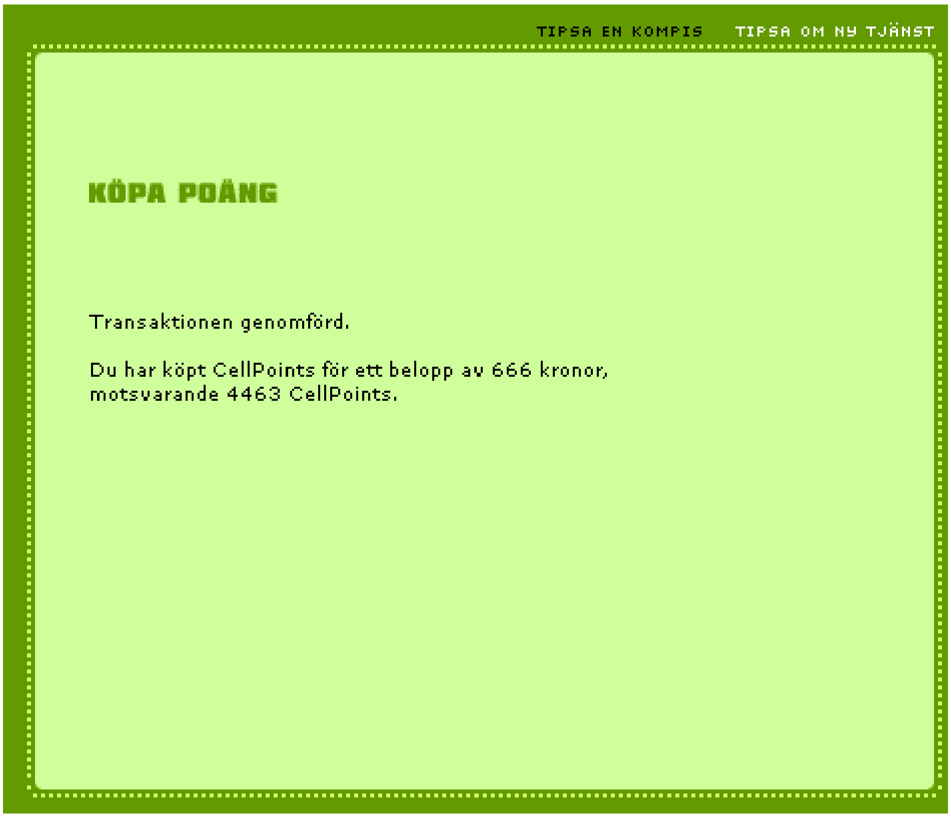
This file makes all payment requests to Netgiro and handles the logging of the transaction. To be able to do that it uses java beans from a package called ppp.

First it checks the data typed in the form, for misspelling etc. This is done locally on the server. No communication with Netgiro is necessary.

If everything is correct a contact to Netgiro is established and a debit request with the specific user data is sent. Otherwise an error page is displayed to the user. See example below.

Depending on the answer from Netgiro either a success page or an error page is displayed to the user.

All communication involving Netgiro is logged in a database. Each transaction has a unique reference number and as much information as possible is stored about the user and the transaction: order id, Netgiro transaction id, transaction result, time, status, user number, user id, amount, points, card number, card type, expire date, user ip address, user browser and OS information.

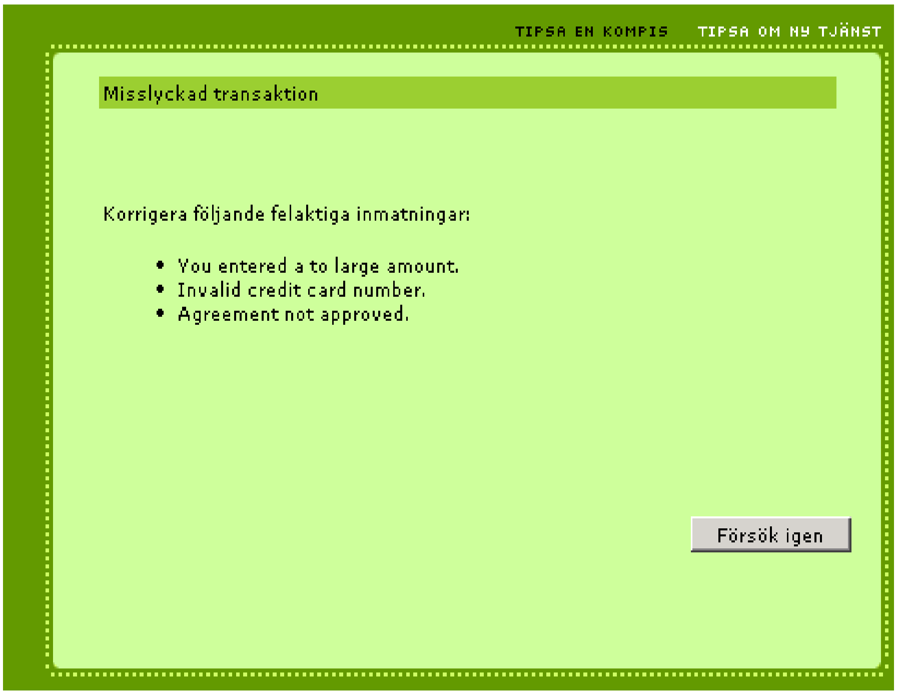


KÖPA POÄNG

Transaktionen genomförd.

Du har köpt CellPoints för ett belopp av 666 kronor, motsvarande 4463 CellPoints.

Figure 12.5. Step 3: The success page is displayed if the transaction went well.

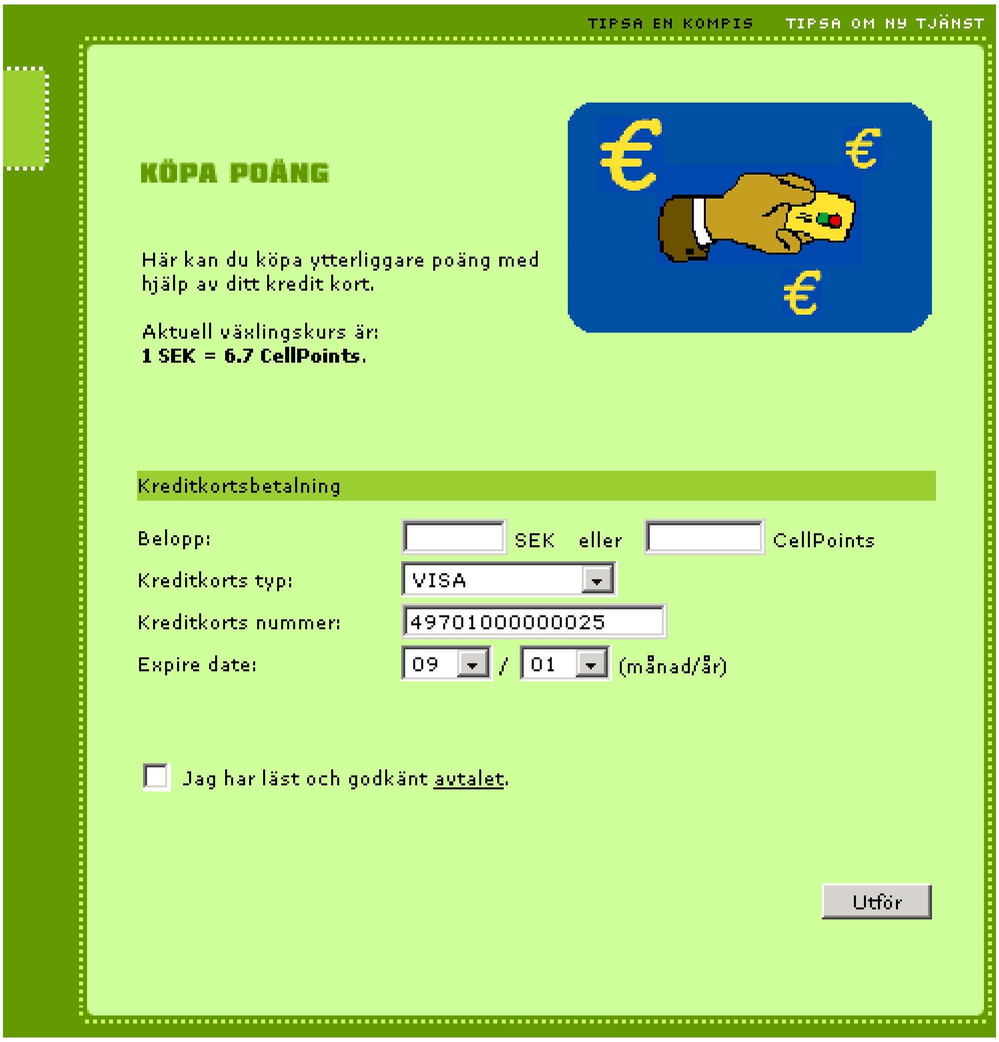


Misslyckad transaktion

Korrigera följande felaktiga inmatningar:

- You entered a to large amount.
- Invalid credit card number.
- Agreement not approved.

Figure 12.6. Failure page. This page is displayed when everything is not ok. In this example the user has entered a too large amount, an invalid credit card number and has not checked the agreement checkbox.



KÖPA POÄNG

Här kan du köpa ytterliggare poäng med hjälp av ditt kredit kort.

Aktuell växlingskurs är:
1 SEK = 6.7 CellPoints.

Kreditkortsbetalning

Belopp:	SEK eller CellPoints
Kreditkorts typ:	VISA
Kreditkorts nummer:	4970100000025
Expire date:	09 / 01 (månad/år)

☐ Jag har läst och godkänt avtalet.

Utför

Figure 12.7. This is how it looks if the user has checked the second checkbox in a previous session (the user has agreed upon storing his/her credit details in the database).

12.2 User Interface – SMS

This chapter describes how the credit card payment possibility can be extended from the wired Internet web case (see section 12.1) to include a mobile way of conducting credit card payments. This solution is based on interactive transactions using simple SMS messages.

This SMS implementation is based on the same back-end payment solution as the web interface described in the previous web section. The difference is how the user interface is connected to the payment system. A big difference between the web and the SMS case is also that SMS has a session-less connection while the user in the web case has the same session throughout the whole payment process. Therefore special arrangements had to be made to be able to bind subsequent messages in the same transaction to each other.

The system architecture is described and necessary components are listed. A user interface has been implemented and the design and functionality is described.

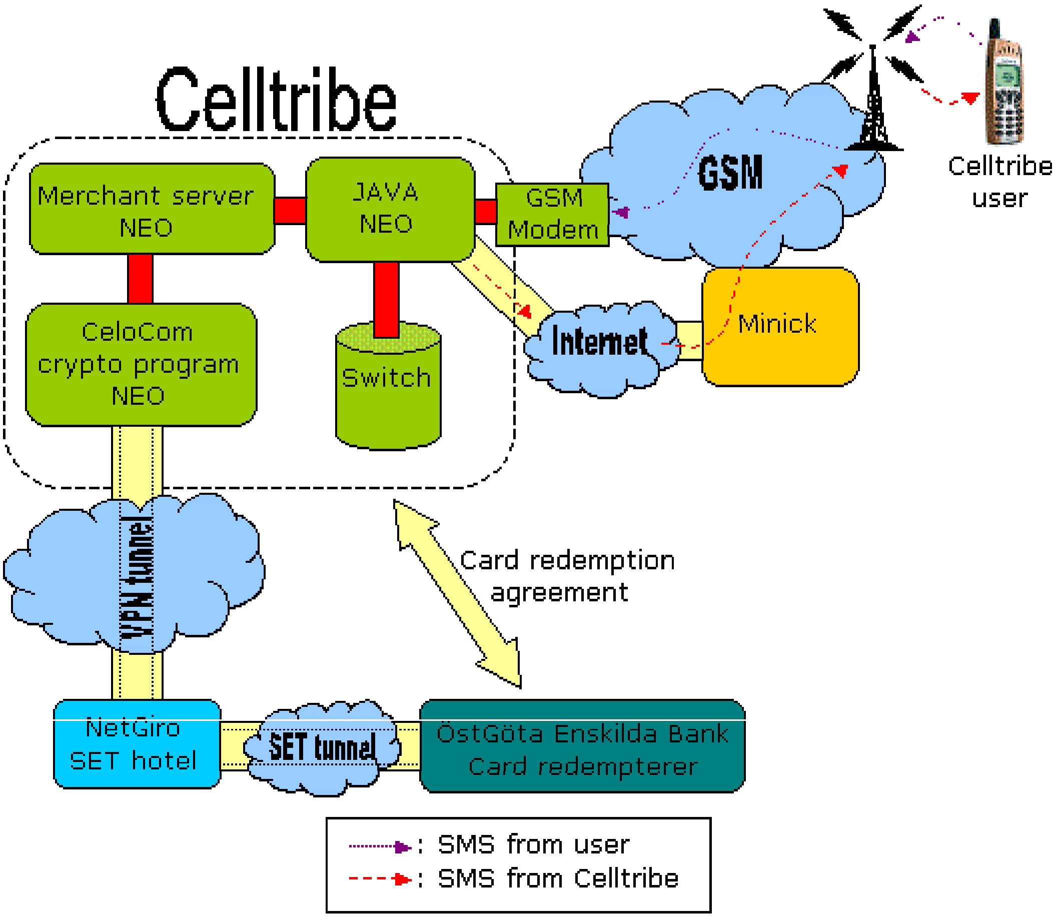


Figure 12.8. Schematic description of the SMS payment implementation.

12.2.1 Description

This product includes three parts:

- Netgiro programs: Transaction classes, Merchant Server and CeloCom encryption server.
- An API, which consists of functions to charge credit cards using the Netgiro payment hotel. And also functions for logging these transactions in a database.
- A working demo/product implemented using Java. Different channels are used for sending respectively receiving SMSes to respectively from the customers.

12.2.2 Netgiro programs

There are exact the same programs and parameters as in the web case. See section 12.1.2 for more information.

12.2.3 Java API

The Java API for the SMS payment system consists of three servers. One server receives incoming SMSs from a GSM-modem. One manager server handles the SMSs and generates the correct response message. And finally one server handles the outgoing SMSs, which are sent over the Internet to a SMSC (Minick).

The total program consist of the following classes in a package called `ppp.sms` (Portal Payment Possibilities with SMS):

Manager server:

- ppp/sms/InterpretSMS
- ppp/sms/Manager
- ppp/sms/ManagerImpl
- ppp/sms/NetgiroPaymentSMS
- ppp/sms/PaymentSMS
- ppp/sms/smsConstants
- ppp/sms/SMSMessage
- ppp/sms/SMSState

Outgoing message server:

- ppp/sms/PPPSmsSender
- ppp/sms/PPPSmsSenderImpl

Incoming message server:

- ppp/sms/Gm12
- ppp/sms/PDUBroken
- ppp/sms/RegGm12

Manager server

The manager server is the main server, which communicates with both the incoming and outgoing message server. To let the servers exchange information between each other RMI objects are used. When the server receives an SMS from the in-server, it tries to interpret the received message. Depending on what data, commands, and numbers, that might be included in the message, the interpret function performs suitable actions and generates a response which is delivered to the out-server.

Incoming server

This server listens to a GSM-modem and whenever the modem receives an SMS the server retrieves it from the modem and decodes the message, which is in hex-code, to regular ASCII strings and sends it on using RMI to the manager server.

Outgoing server

This server handles the connection to the SMSC, in this case Minick, where all outgoing messages are delivered. This server and its send function are called with RMI from the manager server, which in this case acts as client, whenever an SMS is to be sent by the system.

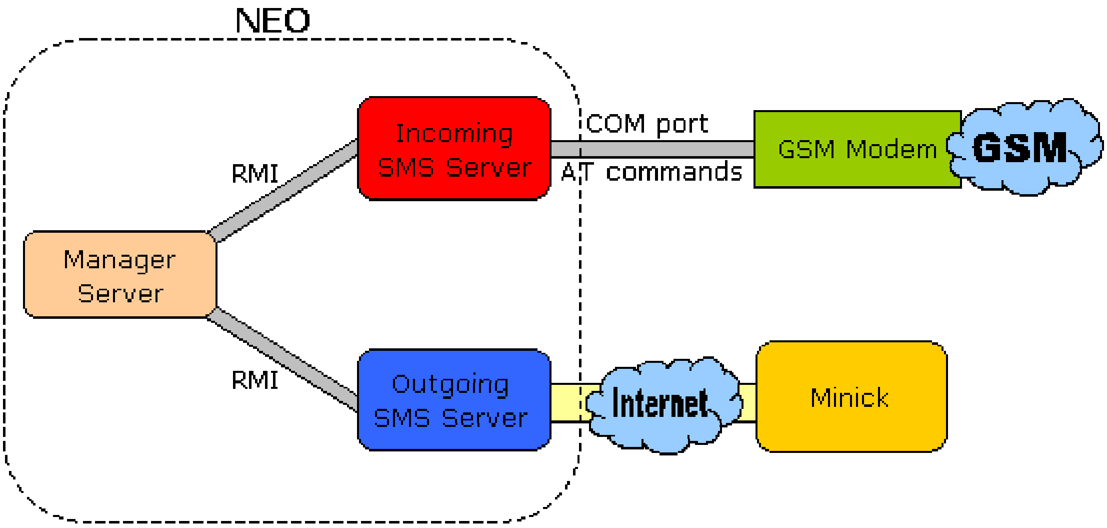


Figure 12.9. Architecture of the SMS payment Java program.

12.2.4 Working demo/product

A payment can be initiated in two ways. The first, and most obvious way is to let the user initiate a certain payment at a specific time. This method is the only one implemented in our product. The second way is via a server initiated transaction that sends a message to the user querying him to make a purchase. This server sent message could use some kind of trigger to know when it should be generated and delivered to the customer. For instance in the Celltribe portal case, the trigger could be when the user's amount of CellPoints sinks below a specific level. To extend our product to this method will not require much effort.

Our product works in the same way as the example described in section 11.1.4 and is illustrated in that section's user interface figure.

The problem with not knowing if a received SMS is the first message in a transaction process or if it is a reply message containing for instance a purchase confirmation means that some kind of a session mechanism has to be used.

Because there is no guarantee that an SMS ever reaches it addressee, problems can arise when a message is lost if one is not using a session id. For example when a user initiates a purchase by sending an SMS to the server, then the server responds with a confirmation request to the user, but suppose that this message gets lost at the operator. Because the user has not received a confirmation he gets tired and sends another purchase request. The server's response now reaches the user. The user confirms the purchase by replying with his code. Now the problem occurs, because the server has no way of knowing whether the confirm message was confirming the first or the last initiated transaction.

The session id also acts as a receipt for the user. Thus, if the user has a complaint about a certain payment, he could use the session id as a reference number for that specific transaction.

The session id is used in combination with a personal code to authenticate the message and also to bind it to the initiating message.

12.2.5 Measurement of SMS delivery

A payment solution using SMS is extremely time dependant. Mobile users of today have developed an everyday habit of sending SMS. In that case the delivery time is of less importance than when utilizing SMS in a bi-directional service. In the latter situation the reliability and delivery time is of extreme importance.

The time factors should therefore be measured. Data collected during previous measurements performed by Celltribe have been used to investigate the delivery time. The data used shows the processing time in Minick. The result from these data can be seen in figure 12.10.

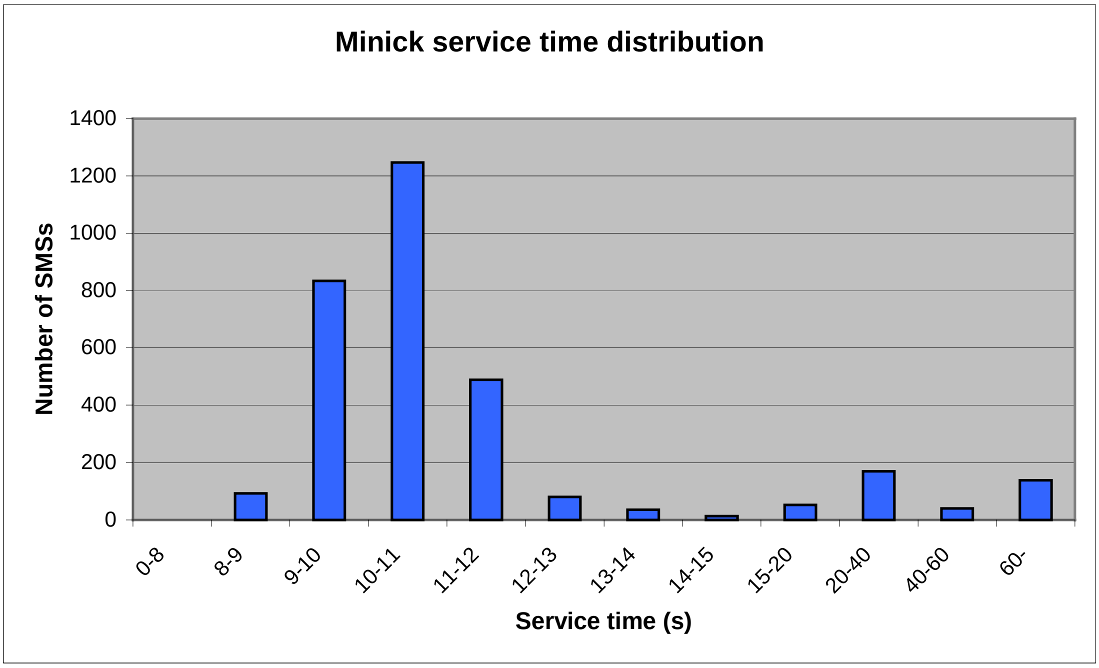


Fig 12.10. Variation of Minick's service time.

When studying these data one can see that most SMS are delayed between nine and twelve seconds. Surprisingly no SMSs are delayed less than eight seconds. The common feeling when testing the implemented SMS payment system was never the less that the above data are not really correct. The impression is that Minick today has a better performance level.

Therefore a measurement was conducted where an SMS is sent through the whole SMS payment system. An SMS was sent from a phone to the GSM modem and the system generated a reply SMS that was delivered to Minick that forwarded it to the phone. In the payment system this is the relevant time since it is the customer's inactivity time while he or she is waiting for a response. The result of these measurements is shown in figure 12.11.

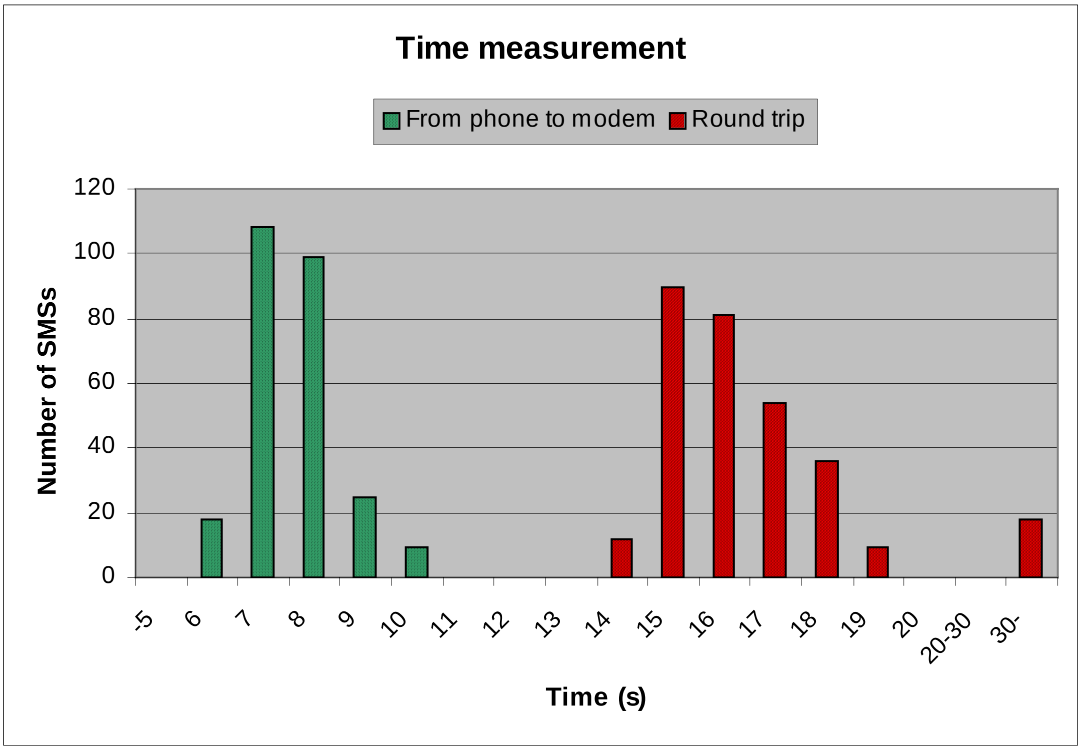


Fig 12.11. Time measurements of the SMS payment service.

The data described in figure 12.11. confirm our suspicions. Under normal load conditions there are no problems using Minick as an SMSC, the small extra time is well compensated for the low price. However, during the last months Celltribe has been having problems with Minick due to over loading. An alternative would be not to use third part like Minick and instead use the GSM modem to send outgoing SMSs when bi-directional SMS services are used.

It would also be interesting to look at the performance level of other competing SMSCs, like for example Wireless Maingate in Sweden, to see if they can guarantee a more stable solution. If that is the case, then the samples with SMSs that take more than 30 seconds in figure 12.11 may be eliminated. Nevertheless, as long as Minick is working properly and does not suffer from over loading the small loss in delivery time is well compensated by the low price per SMS.

13 Future work

This thesis describes the payment solutions available for a start-up company to implement today. However there exist some aspects that would be interesting to follow up. This section describes some of the enhancements that could be interesting to investigate in the area of portal payment possibilities.

13.1 PKI based end-to-end security with payments

This was the original title of the thesis. It is still an interesting subject, but is not feasible for a small company with limited resources to implement any of the hardware solutions that are needed today. Nevertheless the topic is of great importance and with the introduction of for example Java cards that could be updated Over-The-Air (OTA) it might be possible to implement a pure software solution.

13.2 CTI and WAP implementations

Implementing the suggested CTI and WAP solution would be interesting. Performance measurements between the different solutions could be done both on technical aspects but also about the user confidence in each solution. How willing are real users to actually use each separate solution.

In the WAP case security can be further investigated when future WAP versions arrive that might have solved the WAP problems perhaps by introducing new hardware modules in the mobile phone.

13.3 Loyalty points exchange system

Establish connections with several others dealers with electronic currencies and loyalty points forming a virtual exchange service. Such a system would be really interesting. This would be more of a business job, but connecting all the different systems might be interesting.

13.4 Micropayment systems and Jalda

Future investigation of the different micro payment systems, especially the version called wireless Jalda should be watched. This could be done as both a technical and a business investigation.

14 Conclusions

To work in the mobile Internet area in a start-up company like Celltribe, ones priorities shift a lot. The cause of that is probably that the mobile market is now changing rapidly, which relate to the problem of ‘long-time’- planning (several months) in this kind of business. This has definitely reflected the outcome of the report.

The main focus has been to investigate the possible payment methods available. The payment alternatives have been evaluated from Celltribe’s perspective. Therefore a solution involving SIM Application Toolkit (SAT), that would give a high security level, was discarded at an early stage since it is dependent on hardware and reprogramming of customers’ SIM cards.

The best solution for Celltribe would be a combination of two different techniques. For the Swedish web portal the best payment alternative is to implement a direct Internet bank solution, which every large bank in Sweden is offering. However, the direct Internet payment solution is not expandable to the mobile market. Therefore, for the global scenario a credit card solution should and has been implemented. The large advantages with a credit card solution is that it can be implemented for a rather low cost using a third party, like NetGiro, to perform the actual bank transactions. Another large advantage with the credit card alternative is that it does not matter how the credit card information is transferred from the customer to Celltribe. That opens up a lot of possibilities when designing a mobile solution.

The credit card solution was implemented using Java and JSP. The implementation was designed and integrated with Celltribe Mobile Service’s live portal. As the necessary SET engine provider NetGiro was chosen. In that way the market demand can be measured before possibly investing in a SET engine.

A study on how the credit card solution could be expanded to the mobile case has been conducted. The investigation included analysis of CTI, WAP, SMS and dedicated numbers. SMS was chosen over the others, mainly because it fits the company’s profile the best and that ‘all’ Celltribe’s customers are able to use the service. A working credit card payment prototype using interactive SMSs has been implemented using Java.

15 Abbreviations

3DES	See DES
AH	Authentication Header
CA	Certification Authority
CBC	Cipher Block Chaining
CF	Cipher Feedback
CRL	Certificate Revocation List
CSD	Circuit Switched Data
CTI	Computer Telephony Integration
DES	Data Encryption Standard
DNS	Domain Name Server
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptosystems
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards, issued by NIST
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HMAC	Hash function-based MAC
HTML	HyperText Markup Languages
HTTP	HyperText Transfer Protocol
ICV	Integrity Check Value
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange Protocol
IP	Internet Protocol
IPSec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
IVR	Interactive Voice Response
MAC	Message Authentication Code or Medium Access Control
MD5	Message Digest 5
MIA	Merchant Initiated Authorization
NIST	National Institute of Standards and Technology, a division of the U.S. Department of Commerce
NSA	U.S. National Security Agency
OF	Output Feedback
OSI	Open Systems Interconnection
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
RA	Registration Authority
RMI	Remote Method Invocation
RSA	Rivest, Shamir, and Adleman
SA	Security Association
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SHA-1	Secure Hash Algorithm 1
SKEME	Secure Key Exchange Mechanism
SMS	Short Message Service
SMSC	SMS Center
SPI	Security Parameters Index

SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Unified Resource Locator
USSD	Unstructured Supplementary Service Data
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WML	Wireless Markup Languages
WSP	Wireless Session Protocol
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol

16 Bibliography

Here are some interesting documents about the development of the mobile Internet, and also common documentations about e- and m-commerce. Some security publications are also included.

CryptoBytes Volume 2, No. 2 - Summer 1996,
ftp://ftp.rsasecurity.com/pub/cryptobytes/crypto2n2.pdf .

CryptoBytes Volume 4, No 1, Summer 1998 Michael J. Wiener,
ftp://ftp.rsasecurity.com/pub/cryptobytes/crypto4n1.pdf .

Will Cash Go The Way Of The Dinosaur?,
http://www.commweb.com/article/TWB20000816S0018 .

Electronic Money, or E-Money, and Digital Cash, Roy Davies,
http://www.ex.ac.uk/~RDavies/arian/emoney.html .

A quick overview of e-money, 14th March 2000,
http://abracad.users.netlink.co.uk/emoney.html .

Durlacher Mobile Commerce Report, December 1999
http://www.durlacher.com .

The Demand for Mobile Value-Added Services, Nokia 1999,
http://www.nokia.com .

Utvecklingen av Internet - maj 1998/maj 2000, Radio Undersökningar AB (RUAB),
http://www.ruab.se .

Statens Institut för KommunikationsAnalys (SIKA),
http://www.sika-institute.se

Pulling the Internet's Plug, Network Magazine,
http://www.networkmagazine.com/article/NMG20000710S0007 .

The Infinite Monkey Protocol Suite (IMPS), S. Christey, 1 April 2000, RFC 2795.

Mobile Management, The Open Group,
http://www.opengroup.org/online-pubs,

Secure Electronic Transaction: a market survey, Carl Eric Wolrath Sep 1998,
http://www.wolrath.com/set.html

17 References

[1] An Introduction to Cryptography, Ian Curry 1997, http://www.entrust.com/resourcecenter/pdf/cryptointro.pdf, 2000-06-30.
[2]The Internet Key Exchange (IKE), D. Harkins, D. Carrel, November 1998, RFC 2409.
[3] Internet Security Association and Key Management Protocol (ISAKMP), D. Maughan, M. Schertler, M. Schneider, J. Turner. November 1998, RFC 2408.
[4] Security Architecture for the Internet Protocol. S. Kent, R. Atkinson, November 1998, RFC 2401.
[5] Understanding Public Key Infrastructure, RSA Technologies, http://www.rsasecurity.com/products/keon/whitepapers/pki/PKIwp.pdf, 2000-06-25.
[6] Internet X.509 Public Key Infrastructure Certificate and CRL Profile, R. Housley, W. Ford, W. Polk, D. Solo, January 1999, RFC 2459.
[7] Federal Information Processing Standards Publication 180-1 Secure Hash Standard, http://www.itl.nist.gov/fipspubs/fip180-1.htm, 2000-10-03.
[8] The MD5 Algorithm, R. Rivest 1992, RFC 1321.
[9] National Institute of Standards and Technology, http://www.nist.gov/gov, 2000-07-15.
[10] New directions in cryptography, IEEE Transactions on Information Theory 22, W. Diffie and M.E. Hellman, 1976.
[11] Federal Information Processing Standards Publication 46-3 Data Encryption Standard (DES), http://csrc.nist.gov/publications/fips/fip46-3/fips46-3.pdf, 2000-10-01.
[12] RSA Security FAQ What is DES?, http://www.rsasecurity.com/rsalabs/faq/3-2-1.html, 2000-06-30.
[13] Federal Information Processing Standards Publication 186-2 Digital Signature Standard, 2000 January 27, http://csrc.nist.gov/fips/fips186-2.pdf, 2000-07-15.
[14] Use of elliptic curves in cryptography, V. Miller, Advances in Cryptology - Crypto '85, Springer-Verlag 1986.
[15] Elliptic curve cryptosystems, N. Koblitz, Mathematics of Computation 48, 1997.
[16] A method for obtaining digital signatures and public-key cryptosystems, R.L. Rivest, A. Shamir, and L.M. Adleman, Communications of the ACM (2) 21 1978.
[17] CryptoBytes Volume 4, No 1, Summer 1998 Michael J. Wiener, ftp://ftp.rsasecurity.com/pub/cryptobytes/crypto4n1.pdf, 2000-06-24 .
[18]Security Architecture for the Internet Protocol. S. Kent, R. Atkinson, November 1998, RFC 2401.
[19] Internet Security Association and Key Management Protocol (ISAKMP), D. Maughan, M. Schertler, M. Schneider, J. Turner, November 1998, RFC 2408.
[20] The OAKLEY Key Determination Protocol, H. Orman, November 1998, RFC 2412.
[21] VPN BlackBox Technical Report, Team17 2000-05-25.
[22] Security Architecture for the Internet Protocol, Atkinson 1998, RFC 2401.
[23] Baltimore, http://www.baltimore.com, 2000-07-01.
[24] Brokat, http://www.brokat.com, 2000-07-18.
[25] Celo, http://www.celocom.com, 2000-07-15.
[26] ColumbiTech, http://www.columbitech.com, 2000-07-03 .
[27] Entrust, http://www.entrust.com , http://www.entrust.net, 2000-07-18.

[28] GemPlus, http://www.gemplus.com, 2000-07-18 .
[29] Melody Interactive, http://www.melody.se, 2000-07-05.
[30] MESC, http://www.esign-consortium.org, 2000-07-16.
[31] OpenCard, http://www.opencard.org, 2000-07-18.
[32] PKI-forum, http://www.pkiforum.org, 2000-07-13 .
[33] Radicchio, http://www.radicchio.org, 2000-07-15.
[34] RSA Security, http://www.rsasecurity,com, 2000-06-29 .
[35] Schlumberger, http://www.schlumberger.com, 2000-07-18.
[36] SmartCard Forum, http://www.smartcardforum.com, 2000-07-18.
[37] Tantau, http://www.tantau.com, 2000-07-16.
[38] VeriSign, http://www.verisign.com, 2000-08-15.
[39] WapForum, http://www.wapforum.org, 2000-06-28.
[40] WM-data, http://www.wmdata.se, 2000-06-22.
[41] Electric currency could trash cash, C Denny 1999, http://www.guardianunlimited.co.uk/online/story/0,3605,99341,00.html, 2000-08-29.
[42] Survey of Electronic Money Developments 2000, http://www.bis.org/publ/cpss38.pdf, 2000-08-28 .
[43] Beenz, http://www.beenz.com, 2000-08-07.
[44] CyberCash, http://www.cybercash.com, 2000-08-07.
[45] eCash, http://www.ecash.com, 2000-08-16.
[46] Flooz, http://www.flooz.com, 2000-08-14 .
[47] Ipoints, http://www.ipoints.com, 2000-08-08 .
[48] MilliCent, http://www.millicent.com, 2000-08-07.
[49] MyPoints, http://www.mypoints.com, 2000-08-06.
[50] Goyada, http://www.goyada.com, 2000-06-30.
[51] Mobile e-commerce – The new "anytime, anywhere" sales channel, http://www.anuit.it/conv2k04/coiro.htm, 2000-07-29.
[52] Mobile e-commerce – The new "anytime, anywhere" sales channel, http://www.anuit.it/conv2k04/coiro.htm, 2000-07-29.
[53] Ericsson About EDGE, http://www.ericsson.se/edge/, 2000-10-01.
[54] Nokia About UMTS, http://nokia-se.wineasy.se/3g/umts.html, 2000-10-01.
[55] Mobile Commerce Report, Durlacher December 1999, http://www.durlacher.com, 2000-07-28.
[56] Mobile Commerce Report, Durlacher December 1999, http://www.durlacher.com, 2000-07-28.
[57] A quick look at payments on the Internet, EHPT January 2000, http://www.jalda.com, 2000-06-15.
[58] Mobile Commerce Report, Durlacher December 1999, http://www.durlacher.com, 2000-07-28.
[59] Mobile Commerce Report, Durlacher December 1999, http://www.durlacher.com, 2000-07-28.
[60] Utvecklingen av Internet maj 1998/maj 2000, Radio Undersökningar AB (RUAB), http://www.ruab.se, 2000-09-20.
[61] Utvecklingen av Internet maj 1998/maj 2000, Radio Undersökningar AB (RUAB), http://www.ruab.se, 2000-07-29.
[62] Utvecklingen av Internet maj 1998/maj 2000, Radio Undersökningar AB (RUAB), http://www.ruab.se, 2000-07-29.
[63] Utvecklingen av Internet maj 1998/maj 2000, Radio Undersökningar AB (RUAB), http://www.ruab.se, 2000-09-20.

[64] Mobile Commerce Report, Durlacher December 1999, http://www.durlacher.com, 2000-07-28.
[65] Mobile Commerce Report, Durlacher December 1999, http://www.durlacher.com, 2000-07-28.
[66] Pulling the Internet's Plug, Network Magazine, http://www.networkmagazine.com/article/NMG20000710S0007, 2000-07-20.
[67] The Demand for Mobile Value-Added Services, Nokia 1999, http://www.nokia.com, 2000-07-29.
[68] The Demand for Mobile Value-Added Services, Nokia 1999, http://www.nokia.com, 2000-07-29.
[69] The Demand for Mobile Value-Added Services, Nokia 1999, http://www.nokia.com, 2000-07-29.
[70] SET specifications, http://www.setco.org/set_specifications.html, 2000-10-02.
[71] Secure Electronic Transaction: a market survey, Carl Eric Wolrath Sep 1998, http://www.wolrath.com/set.html, 2000-07-15.
[72] Centralen för Elektroniska Korttransaktioner (CEKAB), http://www.cekab.se, 2000-10-01.
[73] GlobeSet homepage, http://www.globeset.com, 2000-07-28.
[74] IBM product info, http://www-4.ibm.com/software/webservers/commerce/paymentmanager, 2000-07-28.
[75] Trintech homepage, http://www.trintech.com, 2000-07-28.
[76] Cekab, http://www.cekab.se, 2000-07-14.
[77] SEB Användarinstruktion Direktbetalning.
[78] SEB Användarinstruktion Direktbetalning.
[79] Handelsbankens Direktbetalning i Handelsbanken.
[80] Föreningssparbanken, Teknikspecifikation för uppkoppling gentemot FöreningsSparbanken Direktbetalning.
[81] Nordbanken e-betalning Installationsmanual, http://www.nb.se/e-betalning/resurs/ehandelmanual.pdf, 2000-10-03.
[82] Jalda homepage, http://www.jalda.com/home, 2000-10-03.
[83] Telia säker handel prislista, http://www.e-commerce.telia.com/tec/butikshandel/download/pris_transaktion.pdf, 2000-10-03.
[84] Sonera Mobile Pay, http://www.sonera.fi/english/solutions/mobilepay/, 2000-08-27.
[85] DebiTech, http://www.debitech.com, 2000-07-18.
[86] KleLINE, http://www.kleline.com, 2000-07-29.
[87] Netgiro, http://www.netgiro.com, 2000-07-19.
[88] Secure Trading, http://www.securetrading.com, 2000-07-23.
[89] WAP forum homepage, http://www.wapforum.com, 2000-10-03.
[90] WAP white paper, AU-system, http://www.wapguide.com, 2000-06-27.
[91] WAP whate paper, WAP Forum, http://wapforum.com, 2000-06-28.
[92] WAP Technical Specification, WAP Forum, http://www.wapforum.org/docs/technical.htm, 2000-06-28.
[93] GSM Technology, http://www.xircom.com/cda/page/1,1298,0-0-1_1-325,00.html, 2000-10-23.

[94] A Brief Overview of GSM, Scourias John, http://kbs.cs.tu-berlin.de/~jutta/gsm/js-intro.html, 2000-10-23.

[95] For more information, GSM 03.40, Technical realization of the Short Message Service (SMS).
[96] For more information, Smart Messaging Specification, http://forum.nokia.com/download/ssm2_0_0.pdf, 2000-11-07.
[97] European Telecommunications Standards Institute (ETSI) homepage, http://www.etsi.org, 2000-10-03.
[98] GPRS white paper, Trillium Digital System, http://www.trillium.com/whats-new/wp_gprs.htm, 2000-07-03.
[99] GPRS Network Infrastructure Dimensioning and Performance, Jim Donahue, BTCellnet.
[100] Mobile Commerce Report, Durlacher December 1999, http://www.durlacher.com, 2000-07-28.
[101] Introduction to CTI, Dialogic, http://www.dialogic.com/products/ctconnct/intro2ct.pdf, 2000-08-17.
[102] Using electronic ID cards – a guide for users and application developers, SEIS 1999.
[103] Using electronic ID cards – a guide for users and application developers, SEIS 1999.
[104] SIM Application Toolkit, Brokat, http://www.brokat.com/int/sms/sim.html, 2000-07-01.
[105] Introduction to SIM Application Toolkit, http://www.wirelesstoolkit.com/intro.html, 2000-07-02.
[106] Goyada, http://www.goyada.com, 2000-06-30 .
[107] Halebop, http://www.halebop.com, 2000-06-28.
[108] IOBox, http://www.iobox.se, 2000-06-28.
[109] Room33, http://www.room33.com, 2000-06-28.