



Mobile Payment

Business Opportunity Analysis
Public White Paper

Version 1.2
November 2007





Mobile Payment - Business Opportunity Analysis

Restricted Information

This document is confidential to the Cyber Dynamix GmbH and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied. Information contained in it must not be disclosed, without the prior written approval of the Cyber Dynamix GmbH. The Cyber Dynamix GmbH does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Copyright Notice

Copyright © 2007 Cyber Dynamix GmbH
Cyber Dynamix is a registered property of the Cyber Dynamix GmbH



Patent-registered No. 10 2005 062 061.2-31 DE
and PCT No. EP2006/008871 & WO 2007/079792

Table of content

1.	Executive summary	4
2.	Background	5
3.	Tango Mobile Payment Service	6
3.1.	Introduction	6
3.2.	How it works	6
3.3.	Overview	9
3.3.1	Sample purchase process	12
3.4.	Highlights	15
3.5.	Research and prototyping	16
3.6.	No Device and SIM impact	16
3.7.	Customer offering and benefits	16
4.	Proposition	17
4.1.	Introduction	17
4.2.	Business drivers	17
4.3.	Key success factors	18
4.4.	Roadmap	19
5.	Payment method and value chain	20
5.1.	Customer	20
5.2.	Mobile Network Operator	20
5.3.	Content Provider / Merchant	20
6.	Conclusions and next steps	21
6.1.	Next steps	21
7.	Acronyms and definitions	22
8.	Contact	23



Mobile Payment - Business Opportunity Analysis

1. Executive summary

Tango Mobile Payment is a Cyber Dynamix led, project initiative, for using mobile phones to make fast, secure payments in a mobile internet based content delivery environment. The secure element in this new payment concept is a new innovative key handling, transaction clearing and approval mechanism.

This innovative payment method does not need retail or point of sales (POS) terminals and works beside them. It could co-exist with new Near Field Communication-Payment Applications and can extent them to all other mobility sales transactions beside POS-Terminals.

The end user can use all available mobile devices, which are web/wap capable and therefore does not need to change the handset or the SIM card. The **Tango Mobile Payment** can be easily adopted by all global network operators and content providers:

- without additional effort at the content provider side
- without additional infrastructure at the network operator side
- without additional interfaces or hardware
- without complex B2B business process integration
- without device or SIM swap

The technology meets the high expectations of customers for simplicity, anonymity and convenience. It is quickly understood and its usage can be readily adopted by the customer.

The **Tango Mobile Payment** provides the content / delivery and mobile industry with a clear pathway to a successful mobile payment service. The opportunity now exists to provide a successful new service for content providers, Mobile Network Operators and MNO customers using the mobile device as a new online payment extension.

2. Background

Cyber-Dynamix GmbH, founded 1999 and located in Nuremberg / Germany, has established oneself in the business areas of system architecture and integration as well as IT - security and project management for mobile applications.

Considerable telecommunication providers, such as E-Plus Mobilfunk, KPN Netherlands, Telefonica SPA and O₂ Germany have hearken back to the many years of experience of Cyber-Dynamix GmbH. Corporation-wide applications, such as design and implementation of the i-mode™ service in Germany, have been realized under the lead management of our company. New mobile applications, e.g. UMTS video streaming, have been jointly conceived and in addition, Cyber-Dynamix GmbH has actively contributed to the introduction of the TV service for mobile devices (DVB-H) at O₂ Germany.

E-Plus Mobilfunk

Portal Security, Consulting
i-mode™, Implementation
Video Streaming, Implementation
Single Sign On, Implementation

KPN Netherlands

i-mode™, Harmonization

Telefonica Moviles SPA

o2 Germany Member of Architecture Group

O2 Germany

i-mode™, Implementation
Video Streaming, Project Management
Service Delivery Platform, Design
DVB-H, Project Management
DVB-H, Techn. Interface to MNO Consortium
DVB-H, Over all Architecture
Single Sign On, Design
Meta Data Repository, Implementation

Beside the business domain *Consulting* the Cyber-Dynamix GmbH operates an own *Open Source* research and technology division. We are evaluating and testing new software components of the *Open Source Community* to provide attractive alternatives to commercial products. These ranges from components like SMS gateways to Telco grade billing solutions. Furthermore, the findings from the technology division provide a basis to realize cost efficient prototypes within "proof of concept" studies.

Tango Mobile Payment therefore is a straight forward result from many years experience in analysing content delivering, billing and end user requirements:

- ease of use
- easy to implement at lowest cost
- secure transactions

3. Tango Mobile Payment Service

3.1. Introduction

During the past years most of the Mobile Network Operators (MNOs) and content providers brought many new services and new mobile applications to the mobile user. The mobile customer faced a lot of different payment methods. He was urged to register himself in numerous non-transparent systems, enter personnel data, credit card number or passwords. Different accounts for different content providers needed to be managed.

Beside the new contactless smartcard technology like Pay-Buy-Mobile, **Tango Mobile Payment** can be used for all Internet shopping, mobile and fixed line access as long as the MNO offers the access technology. **Tango Mobile Payment** therefore could enhance and extend the NFC-mobile payment coverage also to the Internet.

Tango Mobile Payment is designed to enable the mobile customer to shop 1 or 2-click quickly, anonymous, secure, without registering or entering any data in his mobile device.

Tango Mobile Payment is secure, reliable and easy to use. It does not need any special devices, additional software application or new SIM cards on mobile devices. Nearly all existing WAP 2.0 devices are therefore potential candidates to use **Tango Mobile Payment**. It simplifies the adaptation of content providers to MNOs and does not require any proxy or gateway solutions at MNO site. The customers demand for an easy, reliable and trustworthy shopping will be accomplished. No new registration must be performed by the user because **Tango Mobile Payment** is based on the existing contractual relationship (Pre- and PostPaid) between MNO and customer. This strengthens the position of the MNO in the highly competitive Internet market and allows the MNO to offer global payment services including already existing MNO services, e.g. age verification or PIN validation. The content providers must not handle or store confidential personal data (e.g. credit card numbers, address data) simply because the identity of a customer will not be disclosed by the MNO. The digital signed trusted token, issued by the **Tango Mobile Payment** application of a MNO, will act as a 1:1 equivalent for cash for the content provider. By the end of the billing period, the content provider accounts the MNO based on the non repudiated trusted tokens. The **Tango Mobile Payment** solution is robust and insensible against manipulations or replay attacks. Due to the fact, that the purchase process is under the control of the MNO, enhanced analysis in the context of "next best activities" or market research could be performed and a better personalization become feasible. Furthermore **Tango Mobile Payment** could be used by DSL customers in an analogous manner and broaden the service usage to fixed line access too. A MNO - offering DSL as well - will become able to offer a seamless payment service to its customers.

3.2. How it works

The MDP-Protocol (Mobile Devices Payment Protocol) has been developed for easy purchasing and billing of Internet contents, user authentication and anonymous usage in mobile data networks. It is based on the principles of de-centralized provisioning of information, centralized user authentication and certified messages (trusted tokens), which are exchanged between CP (content providers), MU (mobile users) and MNO (Mobile Network Operators).

The communication between a content provider and the mobile user is based on HTTP (RFC 2616), whereas the information is directly transmitted as HTML parameters.

This mechanism is described in the following chapter.

Mobile Payment - Business Opportunity Analysis

The communication between the MU and the MNO is managed most likely over HTTP. SOAP based service requests, which can be initiated from a HTML-page, via an API or an application are feasible too.

“Trusted tokens” (similar to certified cheques) are used for the user’s request authorization. The MNO will authenticate the user, authorize the service usage, charge the user’s account and send a digital signed trusted token via the MU to the CP as an approved statement for subsequent billing.

The MDP-protocol does not need any further online communication between CP and MNO. There is no need for additional components like gateways or access proxies.

The following diagram shows the communication relationship:

A mobile user communicates with the CP via internet. The MNO provides access to mobile Internet. The mobile user will be authorized for payable contents by the MNOs.

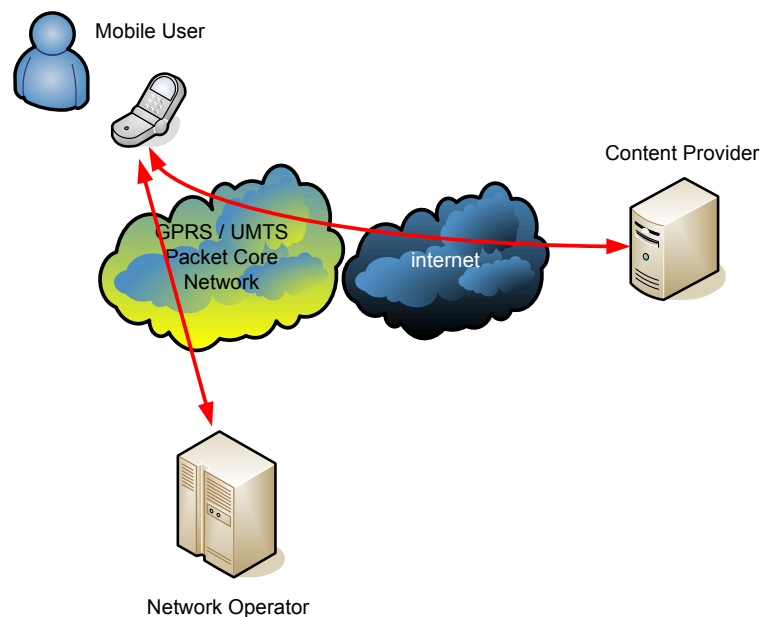


Figure 1: Overview

The following diagram shows the interaction between MU, CP and MNO. Message details are described in the following chapters.

Technical Flow

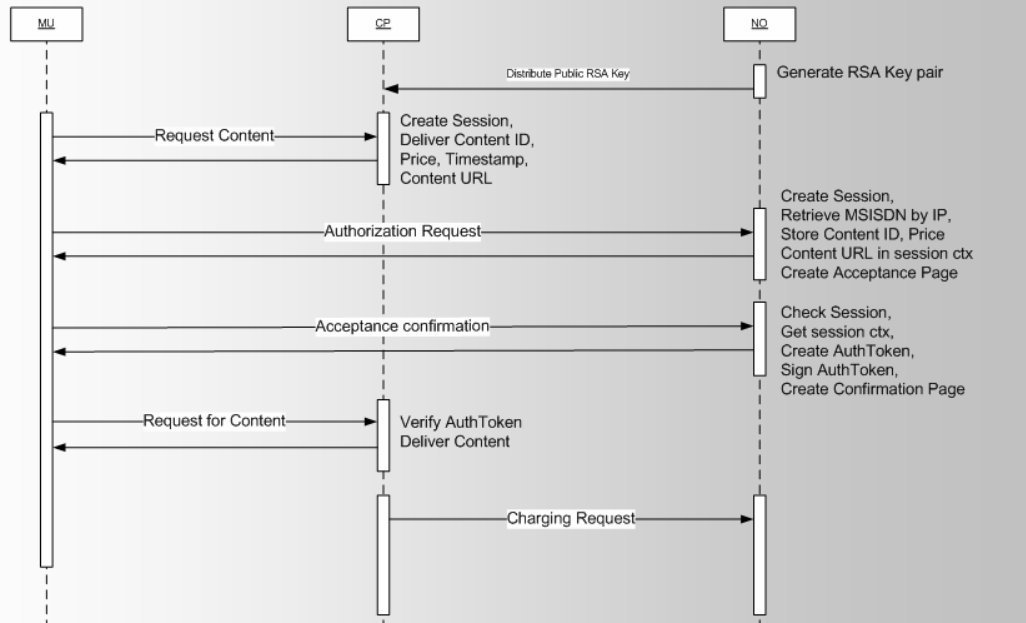


Figure 2: Communication flow

Service authorization:

The mobile user sends a content or service request to a content provider. The content provider does not know the identity of that user but can assign him to a MNO by mapping the IP address to the IP address pool of that MNO. The content provider application will establish a session based context (default web server feature) for storing offer related data during the offer and content delivery process. The content provider responds to the mobile customer with an offer including price, service name, CP- and session-ID for the requested content or service. Once the customer has received the offer on his mobile device, he forwards this offer for authorization and validation to the MNO he is related with.

Mobile User Authentication:

The MNO validates in front of any service usage the authenticity of the mobile customer. The authentication component of the **Tango Mobile Payment application** checks – after having successfully authenticated the mobile customer – the integrity, sanity and plausibility of the forwarded offer data. For that reason, the handed over offer data could be validated against the pre-registered content provider and product repository. If there is any mismatch, an error message is generated and the validation process will be terminated without performing any commercial transaction. In addition, the MNO performs a credit check on the user's Pre- or PostPaid account to ensure, that sufficient balance for the requested service is available.

Content Authorization process

After having performed the logical and syntactical approvals, the mobile customer is asked by the MNO's **Tango Mobile Payment application** if he wants to purchase the good offered by the certain content provider. **At this point, the MNO controls the purchase process.** After having accepted the offer (just one click), the **Tango Mobile Payment application** will digitally sign the approved meta data set and generate the trusted token. During the acceptance process, the mobile customer could be asked for a personal PIN code to pass additional verification levels, e.g. legally required age control in case of adult content. In the next step the **Tango Mobile Payment application** generates a CDR (Call Data Record) for billing purposes. A confirmation response is sent back to the customer that includes the trusted token as HTTP parameter. This specific trusted token is unique, only valid for this particular transaction, bound to the content provider's session ID and acts as a 1:1 equivalent for cash for the content provider.

Mobile Payment - Business Opportunity Analysis

The mobile customer receives the confirmation page including the trusted token. The page informs the customer about the successful purchase process and offers a link to the newly bought content. If the customer clicks that link, the trusted token is forwarded together with the data, stored within the browser context (e.g. session cookie), to the content provider.

The content provider receives that request, and analyses the trusted token. During this process, the digital signature is validated and the hash code of the signed meta data are compared with the offered meta data stored within the session context for this user. If the forwarded (hashed) and stored meta data are identically and the signature of the MNO is valid, the content provider delivers the requested digital good to the mobile customer. The trusted token is stored at the content provider site for later billing purposes. Due to the digital signature, the trusted token could be assigned to a MNO and reflects a non repudiate fact.

After the content provider has delivered the content to the mobile customer, the session must be invalidated and the session context is removed.

At no point of time, the identity of the mobile customer has been disclosed to the content provider. The content provider acts only based on the session ID and the trusted token. In opposite, the MNO has the fully control over the purchasing and billing during the complete sales process

Principles of billing

The content provider is able to generate invoice lists - based on the received tokens - to charge the respective MNO. The MNO uses the MSISDN to assign all authorized services to the respective user. The MNO CDR's are the basis for the settlement between content provider and MNO.

General considerations

Fraudulent manipulation becomes immediately visible by cross checking the transmitted parameters. The RSA signatures ensure a reliable and trustworthy verification of the authorization tokens. Fraud against the MNO authorization systems are unlikely and must happen within the GPRS/UMTS network. The **Tango Mobile Payment** application must not be accessible from the Internet. Fraudulent manipulation against authorization systems are bound to a SIM card. Malicious users can be recognized and barred. Misuse of lost or stolen SIM cards can be blocked by MNOs.

3.3. Overview

The following screenshots are taken from an animated PowerPoint presentation which is embedded in this document. Please click on the symbol below to start the presentation.



Tango
Presentation.pps

Mobile Payment - Business Opportunity Analysis

This presentation highlights the principles of the **Tango Mobile Payment** solution, describes the actors and the interaction between MNO, content provider and mobile customer.

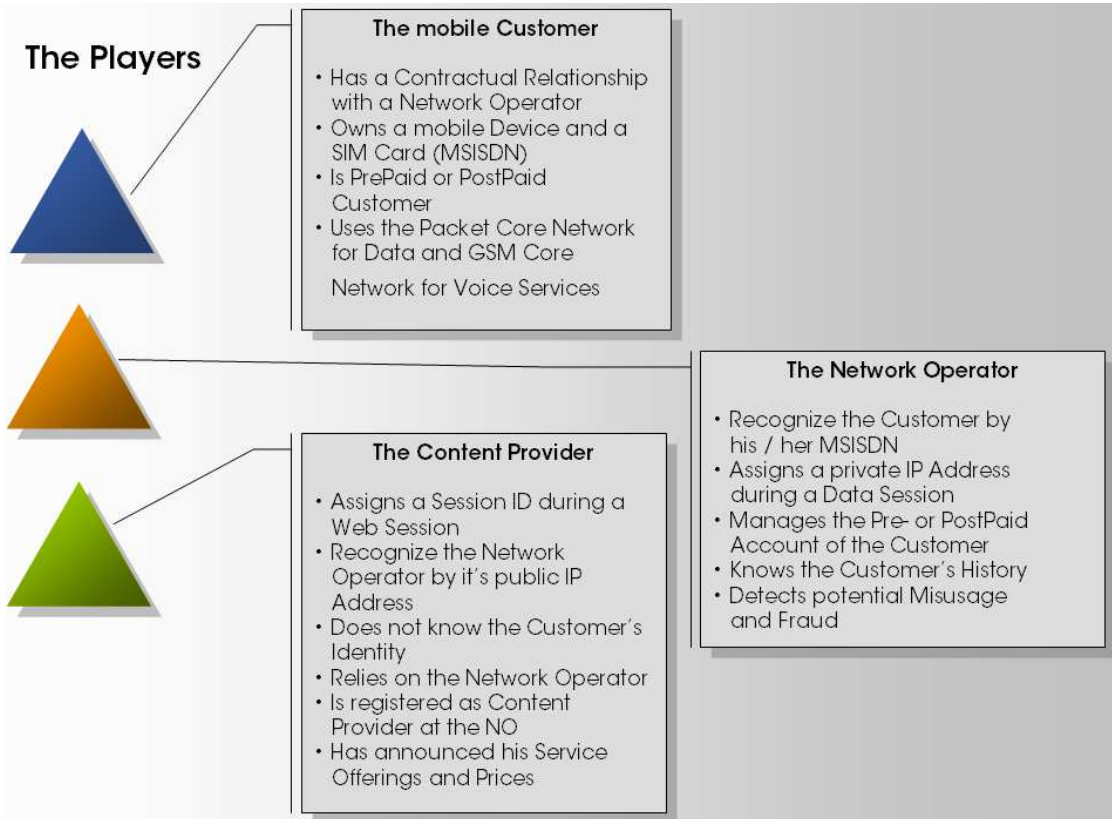


Figure 3: Overview about the players

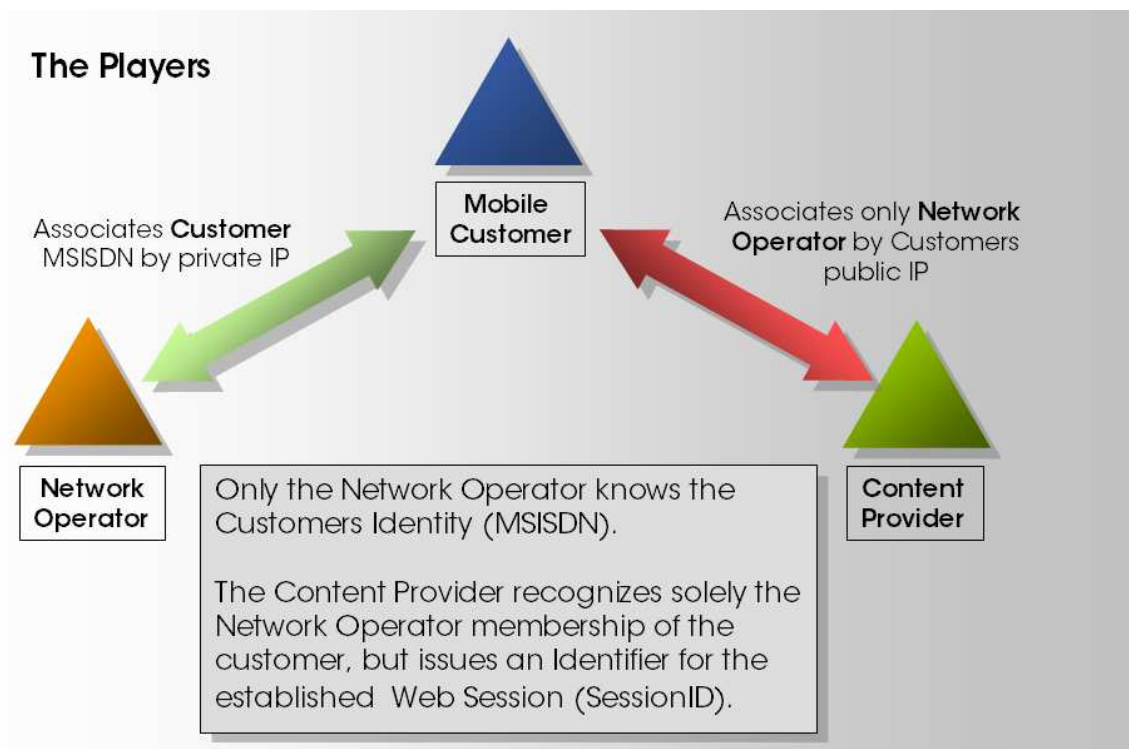


Figure 4: Player's relationship

Mobile Payment - Business Opportunity Analysis

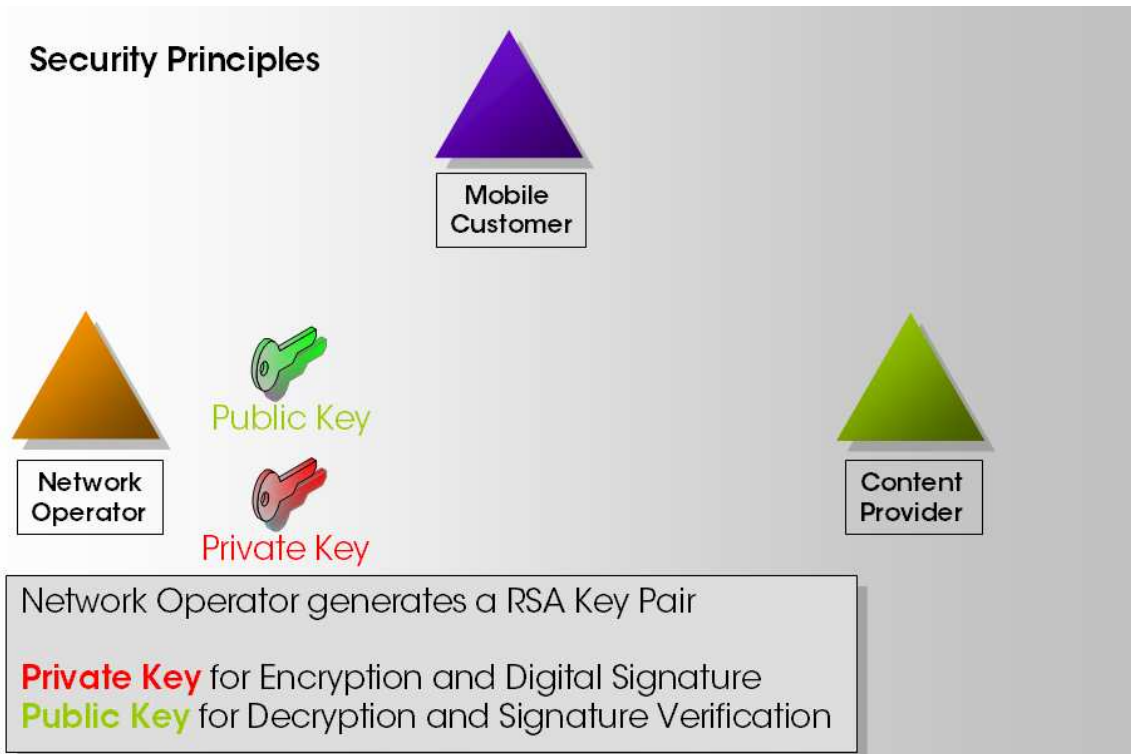


Figure 5: Security principles RSA key

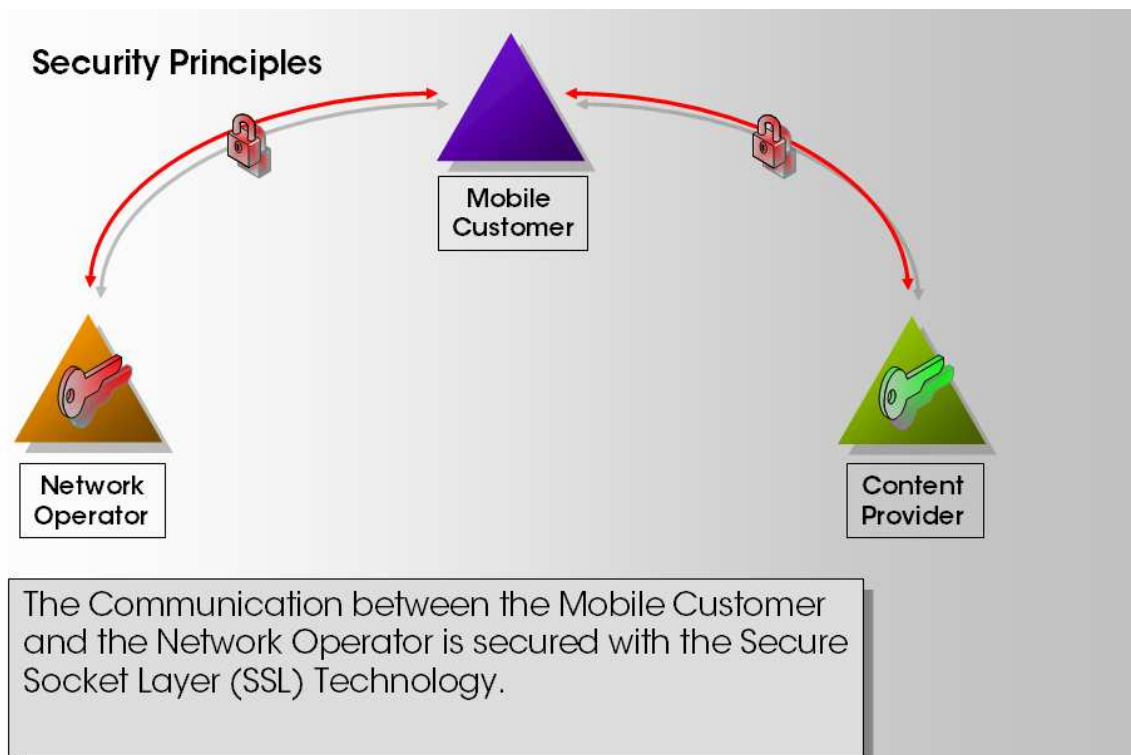


Figure 6: Security principles SSL

Mobile Payment - Business Opportunity Analysis

3.3.1 Sample purchase process

The mobile user found an interesting service

...the content provider initiates a session for him / her.



Figure 7: Tango step1

The mobile user clicks the link "Breaking News" ...

...the content provider responds with an offer.

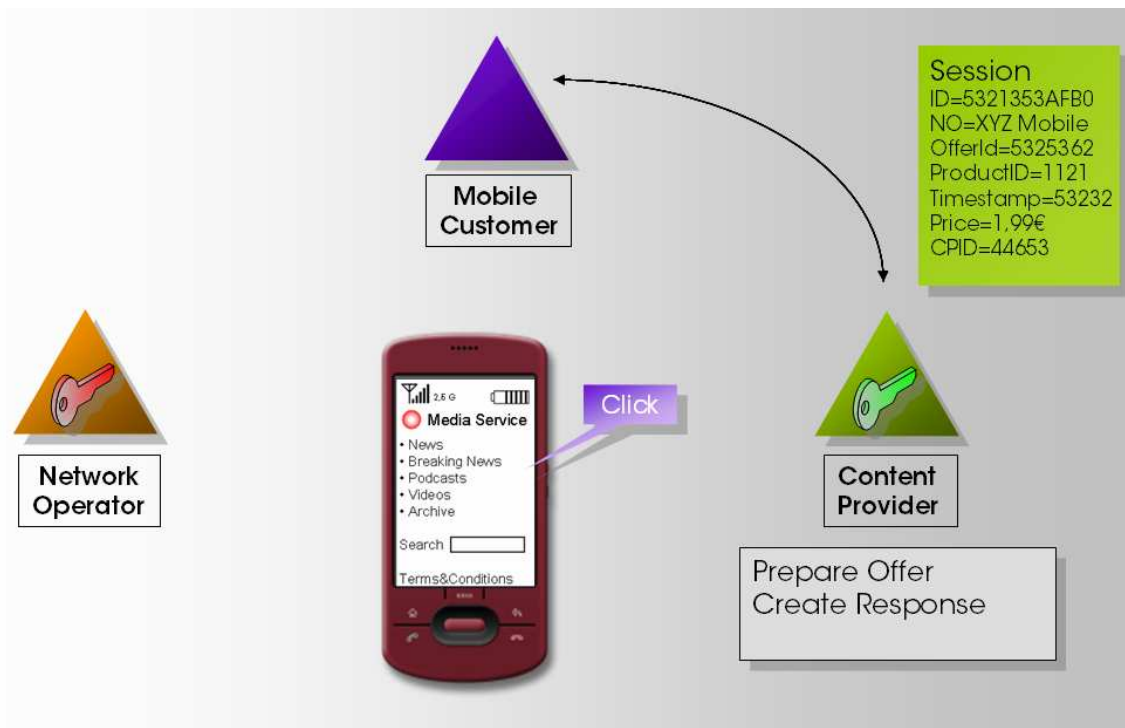


Figure 8: Tango step1a

Mobile Payment - Business Opportunity Analysis

Mobile customer selects the content ...
 ... Tango Mobile Payment application initiates the purchase process.

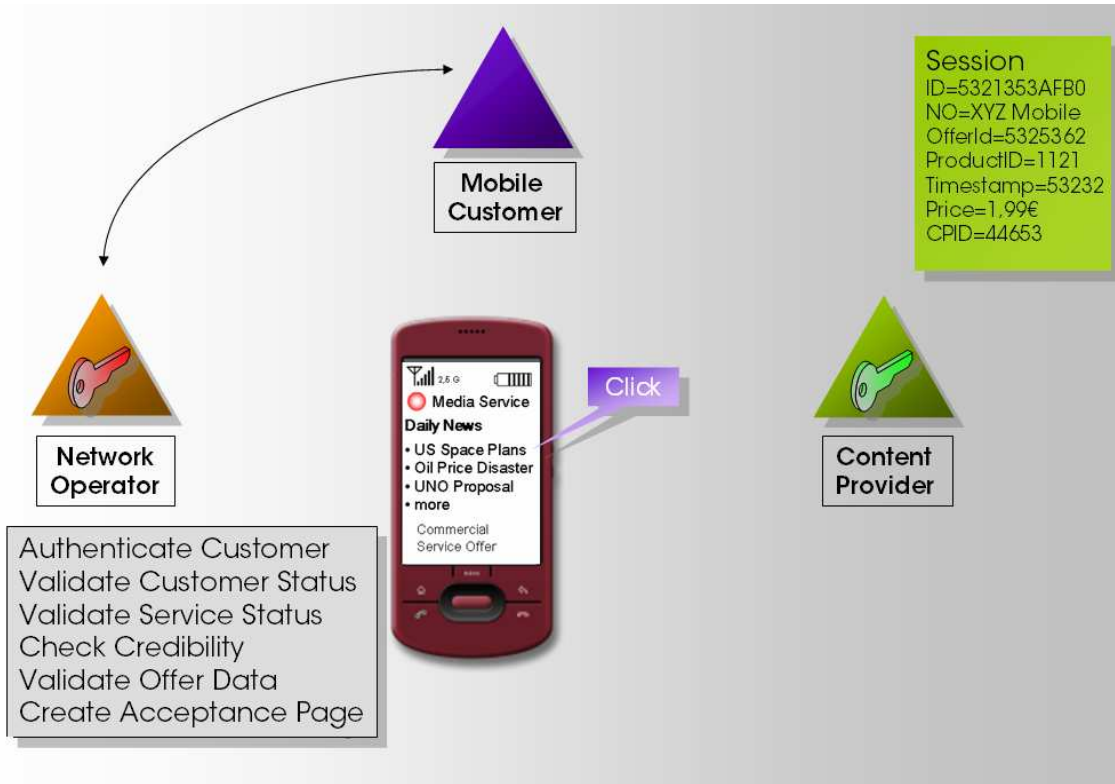


Figure 9: Tango step2

The Tango Mobile Payment delivers the offer, asks for confirmation and the mobile customer agrees on the purchase.

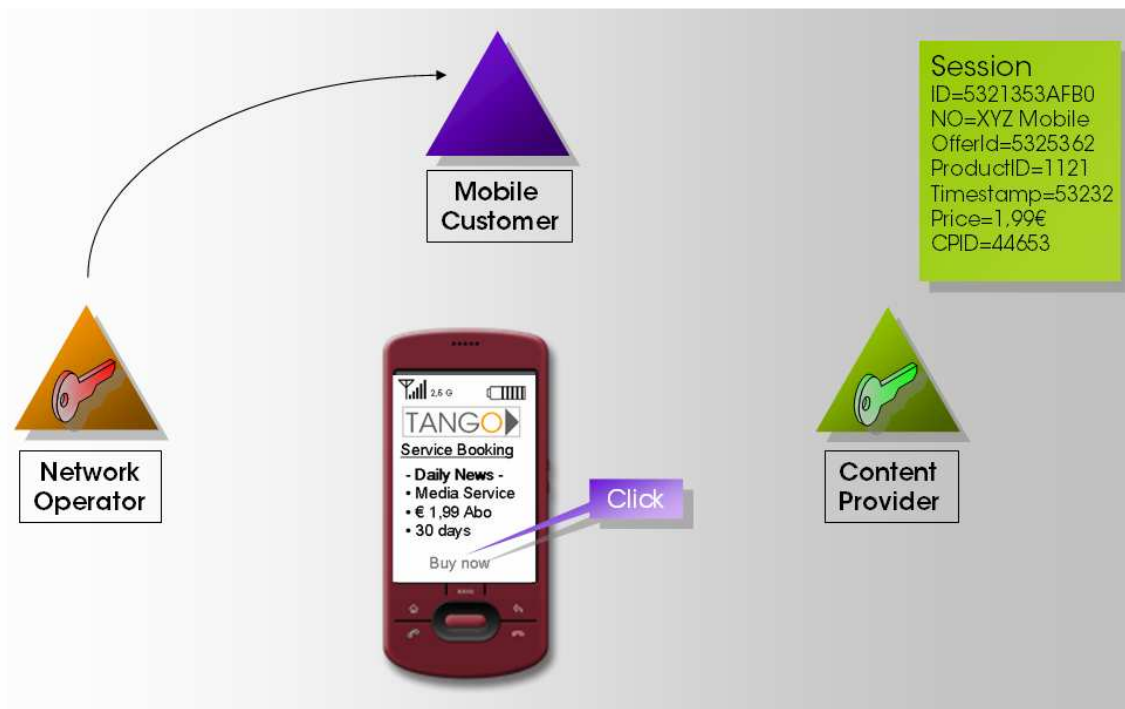


Figure 10: Tango step2a

Mobile Payment - Business Opportunity Analysis

Tango Mobile Payment application finalizes the purchase process, generates the “trusted token” and delivers a confirmation page to the mobile customer.

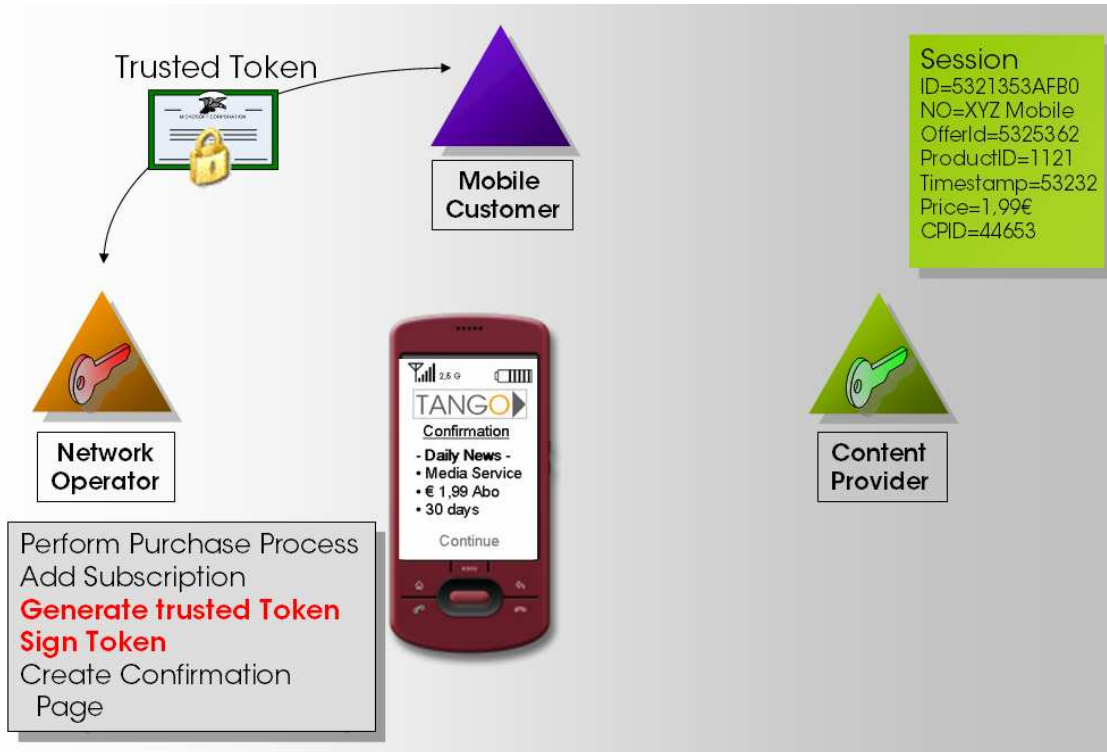


Figure 11: Tango step2b

The mobile customer continues and the “trusted token” is forwarded to the content provider.

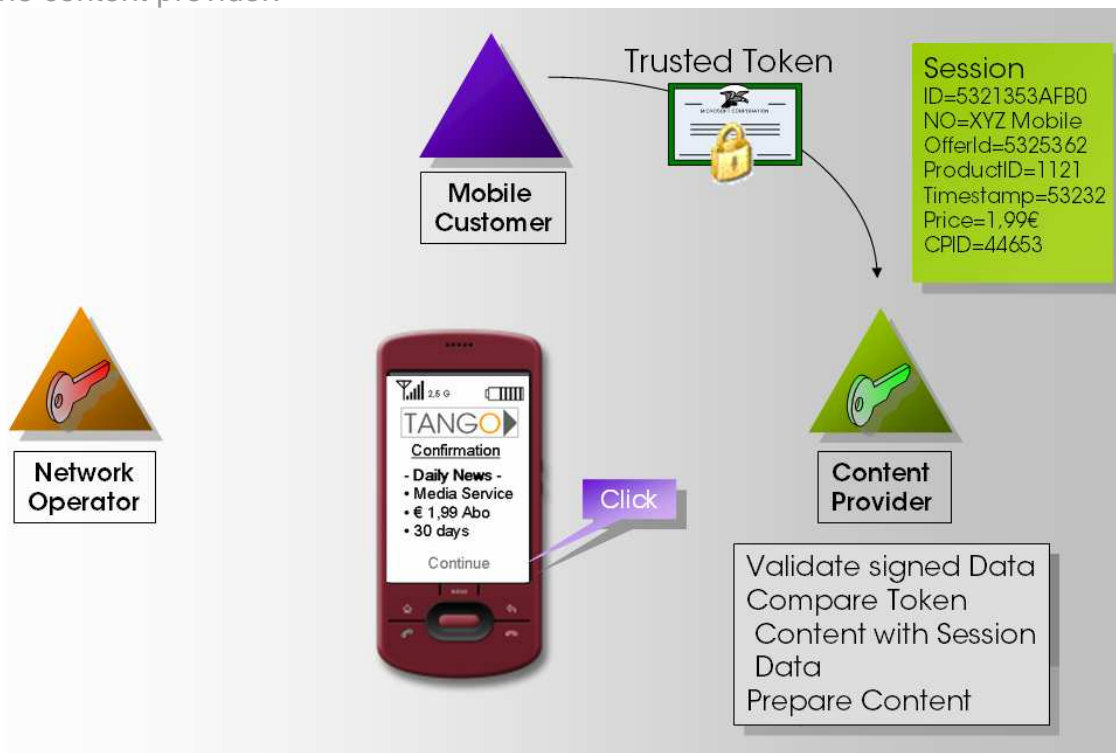


Figure 12: Tango step3

Mobile Payment - Business Opportunity Analysis

After the content provider has delivered the purchased content, the session will be invalidated and the “trusted token” is not valid anymore.



Figure 13: Tango step3a

3.4. Highlights

The **Tango Mobile Payment** solution at a glance:

- Based on Internet standard HTTP (RFC 2616), no additional technology required
- Based on robust and reliable RSA security technology (certificates, encryption and digital signatures)
- Easy to use, transparent and self explaining usage
- Customer's privacy and anonymity is granted
- No dedicated content provider adaptation required
- No business process integration with content providers
- Network Operator keeps the customer relationship
- No repudiation of payment and refunding transaction
- Manipulations become obvious immediately
- Implementation is easy and cost-saving

Mobile Payment - Business Opportunity Analysis

3.5. Research and prototyping

Cyber Dynamix GmbH has developed **Tango Mobile Payment** based on various experiences in the mobile telecommunication industry, service oriented platform design and the in depth understanding in all related business processes. A prototype has been developed for demonstration reason and to proof the security concepts.

CSC Germany has evaluated the **Tango Mobile Payment** solution during a degree dissertation together with the University of Karlsruhe and has taken over the **Tango Mobile Payment** into its own IMDP (Integrated Multi-Media Delivery Platform) product.

3.6. No Device and SIM impact

Tango Mobile Payment will run on every internet capable WAP 2.0 device with a standard web browser.

There is no new development on the UICC/SIM cards or devices necessary.

Tango Mobile Payment works:

- without additional effort at the content provider side
- without additional infrastructure at the network operator side
- without additional interfaces or hardware
- without complex B2B business process integration

3.7. Customer offering and benefits

The mobile customers do not need to:

- change the device
- change the SIM card
- install any additional software on the mobile device
- register for mobile payment
- enter any personal data via the device
- open an dedicated payment account

In opposite, the mobile customer:

- can rely on the MNO (who controls the purchase process)
- can purchase goods completely anonymous
- can comprehend the purchases via his MNO (online) bill
- can perform a 1-2 click quick purchase
- can use his/her PIN issued by the MNO
- can contact a single and familiar customer care instance at MNO side
- can rely on end2end (SSL) security
- can decide whether to provide the content vender with additional data
- can define a credit limit
- can receive additional SMS purchase confirmations
- can use one single payment method for all kinds of content and access channels (SMS, WAP, streaming, download, broadcasting, ...)

4. Proposition

4.1. Introduction

The **Tango Mobile Payment Solution** provides the content / delivery and mobile industry with a clear pathway to a successful mobile payment service. The opportunity now exists to provide a successful new service for all kind of content- and Internet service providers, MNO's and MNO customers using the mobile device as an easy web/WAP based new payment extension.

Cyber Dynamix GmbH will provide a business model that is applicable in any particular market and can flexible vary from country to country or MNO to MNO dependent on the commercial environment, regulatory obligations and technical infrastructure.

Nevertheless, Cyber Dynamix GmbH sees that opportunities for **Tango Mobile Payment** solution in most countries around the world.

4.2. Business drivers

The main business drivers for **Tango Mobile Payment** are:

- *Speed up and convenient usage leading to higher transaction volumes:*
Tango Mobile Payment offers a quick and convenient method for mobile purchasing of goods and internet offers and gives customers an opportunity for a secure, reliable anonymous purchasing based on the contractual relationship between MNO and customers. Research has suggested that the anonymous and secure payment will actually stimulate additional revenues, particularly low-value transactions.
- *Differentiation:*
Billing of all **Tango Mobile Payment** transaction is done by the MNO only. The content provider does not need to implement new billing processes and can save all billing related efforts. Furthermore, the MNO stays in the driver seat of commercial activities of its customers and can analyse the purchase behaviour to optimize cross and up selling potentials. The additional information leads to a higher personalization rate for other mobile services (e.g. portal based offers) and to stimulate the customers demand.
- *Customer's privacy and anonymity:*
Tango Mobile Payment will offer the customer a secure access to the MNO's and content provider products. The customers are only known and billed by MNO's but they can stay anonym to the content providers as long as s/he wishes. If the purchase is on digital download goods only, e.g. news, ring tones, videos etc. there is no need to register or send personnel data. The customer can allow the MNO to send additional personnel data (e.g. necessary delivery name, address)
- *Cost of management:*
The life-cycle total cost of ownership for operating **Tango Mobile Payment** will, potentially, be less than the operational costs of payment cards in the long term. The mayor benefit is that no costs for a SIM swap or new devices will appear. The legacy equipment could be used. Due to the fact, that no additional interfaces of content providers must be implemented or business processes must be adapted, the monitoring, surveillance and administration costs are significant lower than comparable solutions.

Mobile Payment - Business Opportunity Analysis

- *Infrastructure investment:*

Tango Mobile Payment is based on standard internet technology, e.g. HTTP, SSL. The investment will only cover new secured web and applications server and the **Tango Mobile Payment** application. The backend integration is simple, because existing business processes e.g. IN payment or CDR generation will be used.

- *Risk management:*

Man-in-the-Middle – The use of end2end SSL/TLS connections between mobile user and content provider as well as mobile user and MNO prevents a Man-in-the-Middle attack.

Replay attack – The content provider generates a temporary session-ID which is tidily coupled to the access information, preventing replay attacks. The session will be invalidated after a successful content delivery.

Reproduction of tokens – The use of RSA encryption makes it impossible to reproduce a token. A potential fraud would need the private key which is stored at a secure area within the MNO and protected against unauthorized access.

Identification of the mobile user – An identification / recognition of the mobile user by the content provider is not possible because no personal data as MSISDN, XID or any recurring information is send to the content providers.

Fraud by parameter manipulation – Each participating content provider needs to register once at the MNO.

Therefore it's possible to run on all transferred data a plausibility check. A potential manipulation can be detected and the authorization process will be cancelled. The content provider can only recognize the related MNO of the mobile user.

Fraud by faked token parameters – The content relevant information is stored at the content provider site, and is not tied to the transmitted "trusted tokens". A token parameter manipulation is therefore visible to the content provider and the content delivery can be prevented.

Fraud by faked content provider's billing parameter – The content provider's billing records will be checked against the MNO authorizing data records. Any mismatch will be recognized and sorted out.

- *Reduced service delivery time:*

Service / content purchase and delivery time is now fully independent of the browser timeout time (preset 60seconds). Due to the fact that no registration and other transactions between content provider and MNO are needed, the complete purchase to successful delivery time is dramatically reduced.

4.3. Key success factors

In order to **Tango Mobile Payment** to be successful, the following facts need to be addressed:

- *Value for all mobile payment members:* The content provider, Internet shop and merchants associated to the **Tango Mobile Payment** solution will not need to install additional hardware or software. They just use common interfaces. The MNOs can easily integrate a **Tango Mobile Payment** server at moderate costs.



Mobile Payment - Business Opportunity Analysis

- *Large customer base:* **Tango Mobile Payment** can easily take off as the MNOs are able to reach their large customer base.
- *Customer trust:* Will be built on the existing contractual relationships between a client and his MNO.
- *Avoid fragmentation:* Differing and incompatible technical solutions would lead to fragmentation, and so there is a need to standardize the **Tango Mobile Payment** implementations.
 - Inter-operability: appropriate standardization is essential in order to provide convenient and cost-effective **Tango Mobile Payment** services
 - The **Tango Mobile Payment** application and server hardware at the MNO site need, therefore, to be standardised to ensure that, wherever possible, they are able to operate anywhere around the world.
- *Partnership:* Cooperation between MNOs, Internet service and content providers will be essential for the success of **Tango Mobile Payment**. It will generate new business opportunities and values, and does not challenge existing (pay or credit) card transaction businesses.
- *Certification:* The **Tango Mobile Payment** solution has been designed to satisfy all of the known requirements of the MNOs, payment scheme and the Internet service and content providers.

4.4. Roadmap

The roadmap for the introduction and implementation of **Tango Mobile Payment** will depend on the following factors:

- Introduction of **Tango Mobile Payment** services by the MNOs
- **Tango Mobile Payment** server integration into MNO's infrastructure
- Standard contracting of Internet service and content providers and MNOs
- Acceptance of **Tango Mobile Payment** by the mobile subscribers

5. Payment method and value chain

This chapter describes the roles and responsibilities of the key players within the **Tango Mobile Payment** system and value chain. The **Tango Mobile Payment** solution is incorporating the following players:

- Customer
- Mobile Network Operator
- Content provider, service provider, internet shops, ...

No significant change is anticipated to the existing MNO billing infrastructure and processes. The role of the various players in the new payment solution is briefly described below.

5.1. Customer

The **Tango Mobile Payment** customer is required to be a subscriber of a mobile network operator. The mobile customer is required to have an account at the MNO. The mobile customer enters into a service agreement with the MNO for the **Tango Mobile Payment** service.

The mobile customer

- has a contractual relationship with a MNO
- owns a mobile device and a SIM card (MSISDN)
- is PrePaid or PostPaid customer
- uses the GPRS/UMTS packet core network for data and GSM core network for voice services

5.2. Mobile Network Operator

The mobile network operator (MNO) owns the key role and is required to enable **Tango Mobile Payment**. The role of the MNO is to:

- provide and maintain the network infrastructure that enables the secure setup of the **Tango Mobile Payment** server
- provide the customer, via the **Tango Mobile Payment** server, the trusted and certified token
- provide mobile services customer care
- manage the billing to the customer
- provide the interface to the merchants and content providers

The MNO correlates the assets of a mobile customer base and network infrastructure.

5.3. Content Provider / Merchant

The content provider or merchant is the provider of goods and services being purchased by the customer via the mobile internet. The content provider or merchant has a contract with the MNOs in order to clear the monthly settlement.

The content provider:

- assigns a session ID during a Web session to a mobile customer
- assigns the Network Operator by the public IP address of the mobile customer
- does not know the customer's identity, relies on the Network Operator
- has been registered as content provider at the MNO
- has announced his service offerings and prices

6. Conclusions and next steps

6.1. Next steps

The next planned steps for the **Tango Mobile Payment** project are:

- Increase the publicity for the **Tango Mobile Payment** project in order to begin to raise awareness of the capability and make prospective stakeholders aware of its value.
- Use the excellent GSMA network to arouse interest in the MNO community.
- Find a prospective MNO for a trial. This pilot will demonstrate the validity of the technical solutions and determine the customer behaviour jointly with the content providers.
- Identify enhancements/requirements based on the outcome of the trials and work on standardization aspects.

7. Acronyms and definitions

Acronym meaning

API	Application Programming Interface
BSS	Business Support Systems
CDR	Call Data Record
CP	Content Provider
EMV	Europay, MasterCard and Visa
GPRS	Global Packet Radio Standard
GSM	Global System for Mobile Communication
GSMA	GSM Association
HTML	Hypertext Mark up Language
HTTP	Hypertext Transfer Protocol
IMDP	Integrated Multi-Media Delivery Platform
IP	Internet Protocol
MDPP	Mobile Devices Payment Protocol
MNO	Mobile Network Operator
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MU	Mobile User
NFC	Near Field Communication
OTA	Over The Air
PIN	Personal Identification Number
POS	Point of Sale
RFC	Request for Comment
RSA	RSA Cryptographically Method
SIM	Subscriber Identity Module
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
UMTS	Universal Mobile Telecommunication System
WAP	Wireless Access Protocol
XID	Anonymous Identifier ("Mister X")

8. Contact

For additional information please contact:

Gerhard Feder
gerhard.feder@cyber-dynamix.de

Cyber-Dynamix GmbH
Gesellschaft für Systemintegration mbH

Heiner-Stuhlfauth-Str. 28

90480 Nürnberg

Tel: +49 911 / 180 91 05
Fax: +49 911 / 180 91 09

<http://www.cyber-dynamix.de>