ipacri romania

9, Crisana Str.; 70 783 Bucharest 1, Romania; Tel/Fax: +(40-1)212 65 95; office@ipacri.ro; www.ipacri.ro

mSignature Solution
For Wireless Applications
An Overview
IPACRI Romania

White Paper

CREATED BY:
MIRCEA GHIDARCEA

DATE:
21TH MAR 2002

Summary:

This document indents to manifest IPACRI Romania's solution for digital signature in the context of today's Romanian existent implementations of wireless communication.

CONTENTS

1 Introduction

More than 3 million wireless devices are in use at the moment in Romania. Most of them are GSM phones, not enabled for WAP or GPRS.

M-banking has been a subject of high interest for the leading banks of Romania as well as for smaller but dynamic banks looking to acquire a base of sophisticate, demanding and rewarding Romanian clientele. However, due to pour security provided by the existing phones and slow, unpractical use of the applications based on GSM technology, the m-banking has not succeed to become a real distribution channel for banking services.

If m-banking is still a target for the banking industry, the m-commerce has not even started to be debated in other industries.

GSM operators have pushed the notion of mobile Internet offering WAP based services. Despite of the effort and money spent in promotion, consumers have recognized soon that WAP is not Internet. The lack of communication between WAP area and Internet applications has made them to reject the offer made by GSM operators.

Companies and individuals are willing to extend in the wireless space if their business requirements are met, with a special accent on security issues.

Starting with December, 2000, Romania becomes the first country in Europe and one of the first in the World to embark on the road to the 3rd generation mobile telephony. For the first time the promise of a secure, fast and reliable mobile Internet has been fulfilled by Telemobil through its new, innovative Zapp Mobile service, based on CDMA 2000 technology.

The authentication of the parts involved in an electronic wireless transaction and of the data itself is a major problem.

This problem can be solved using digital signatures.

The Romanian Law on e-signature provides the legal framework for a highly secure m-commerce.

IPACRI Romania has developed a solution for digital signature in the mobile world.

1.1 *Scope*

The scope of this document is to explain IPACRI Romania's solution for digital signature and prove its feasibility, reliability and compliance with the law framework and general business requirements.

2 Business Requirements

Service providers want:

- to be sure that the received requests are really issued by that customer that the end-user claims to be
- to be assured that the data received haven't been tampered with on the route from the end-user to the service provider
- to have a way to prove that they indeed receive that specific data/request from the customer and that the request have been made at a specific date/time
- to minimize the impact the implementation of such a solution has upon their existent applications and its intrusion in the data flow between them and their customers

End-users want:

- to be sure that the interlocutor is really the service provider that he is expecting to talk to
- to be assured that the data sent by him in not tampered on the route to the service provider
- to have a way to prove the request sent by him had a specific content and was issued at a determined date/time
- to ensure its privacy by minimizing third parties intrusions in its conversations

All the problems above can be solved using digital signature and time stamps for data exchanged over wireless networks.

Wireless operators want:

- to raise the level of data traffic through their infrastructure by providing a way to support secure transactions
- to minimize the impact such a solution has upon their existent infrastructure

An implementation of a general digital signature/time stamp solution would help the operator to attract more business on his network, and the operator would be especially happy with a solution that requires a minimal effort from his part.

IPACRI Romania is now providing such a solution.

3 IPACRI Romania's mSignature Solution

3.1 *mSignature Service concept*

An ideal digital signature solution would involve the signing of the message and the authentication of the interlocutor using the local resources of the wireless device. This approach is not possible at the moment because of the lack of support from device manufacturers in implementing open security features on their devices. Such security mechanism can be implemented, on SIM based devices, with a SIM Toolkit approach, but such a solution looses generality and is quite difficult to propagate to the mass of the mobile users. More, for the existent CDMA phones this is not an option.

Another approach would be to use the capabilities of the browsers that reside on most phones at this moment, but those capabilities are very poor, if they exist at all.

Meanwhile, while waiting for the browsers to evolve or for the manufacturers to agree upon and implement general mechanism to develop solutions on their devices, a device independent path had to be taken in order to solve the problem and provide this kind of service.

The solution is to provide this service not from the device, but from an independent mSignature Service that has all the capabilities required, as they emerged above, but still provide the appropriate privacy.

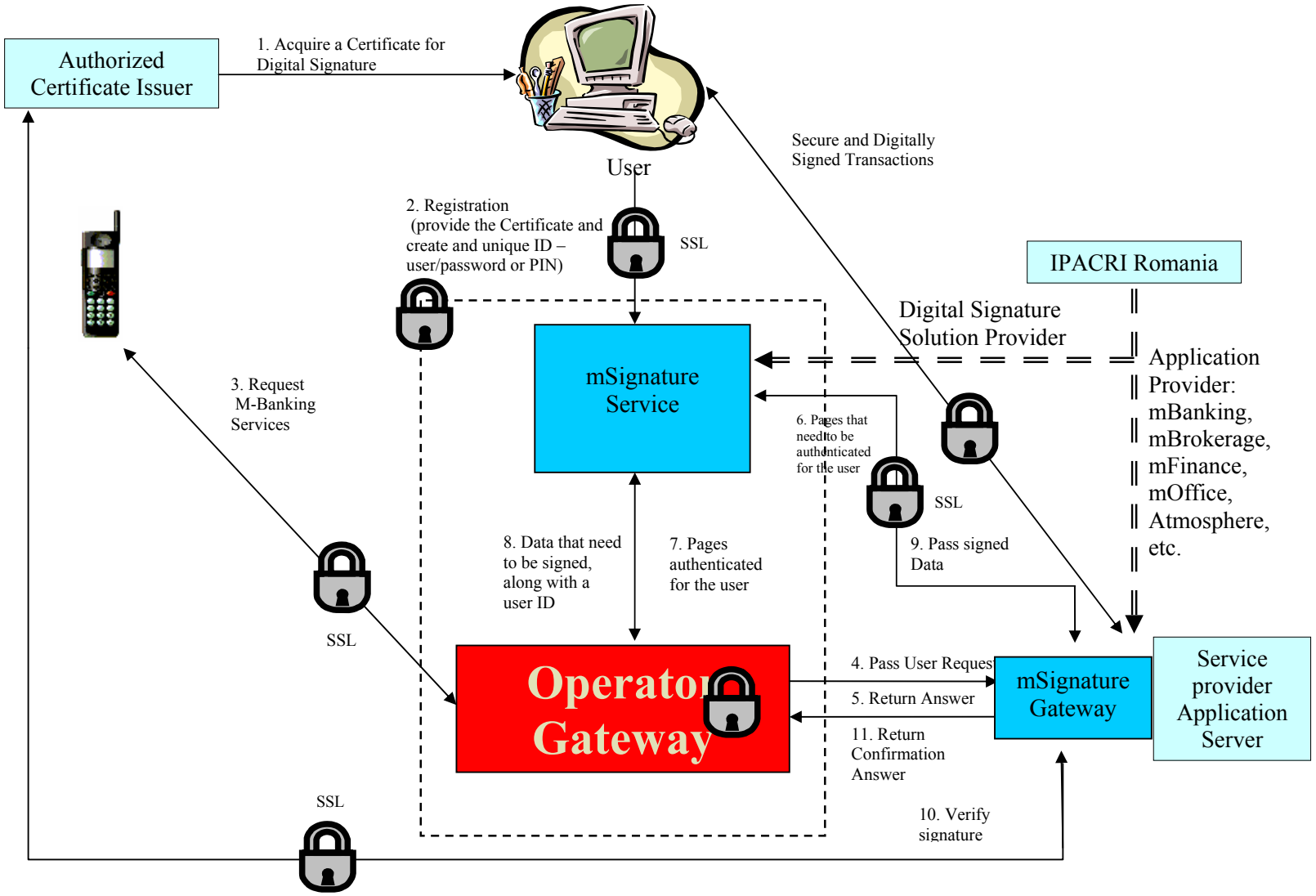
Such solutions are encouraged by organizations like Certicom, with a PKI Gateway that acts very much like our mSignature Service, Mobey Forum, proposing a proxy based solution, or even SET, promoting a solution involving a payment gateway.

3.2 *Architecture*

IPACRI Romania has devised an architecture based on the concept of a mSignature Service that functions as a trusted third party signer on behalf of the end-user. This Service will also authenticate for the end-user the interlocutor he is discussing with.

The end-users and the service providers that require signature services will register with the mSignature Service by providing their identification data and digital certificates (including the private keys for end-users, so that the Service can sign messages on their behalf). The Service will sign data incoming from end-users and authenticate the pages served by service providers.

The mSignature Gateway or a set of libraries and APIs are provided to service providers in order to enable their applications for digital signature.


Authorized Certificate Issuer
1. Acquire a Certificate for Digital Signature
User
Secure and Digitally Signed Transactions
2. Registration (provide the Certificate and create and unique ID – user/password or PIN)
SSL
IPACRI Romania
Digital Signature Solution Provider
Application Provider: mBanking, mBrokerage, mFinance, mOffice, Atmosphere, etc.
mSignature Service
3. Request M-Banking Services
6. Pages that need to be authenticated for the user
SSL
9. Pass signed Data
8. Data that need to be signed, along with a user ID
7. Pages authenticated for the user
SSL
Operator Gateway
4. Pass User Reques
5. Return Answer
11. Return Confirmation Answer
mSignature Gateway
Service provider Application Server
SSL
10. Verify signature

3.3 *Main functionalities*

3.3.1 Data signing

The process of data signing was designed in order to assure a maximum of functionality and privacy with a minimum of interaction with the end-user. The underlaying principles used are:

- the end-user must be in control of the data to be signed at all time
- the service provider must verify that the data signed is the data intended to be signed by the end-user.

In order to satisfy all of the above requirements we came up with the following process, described bellow through its steps:

1. The end-user is filling and submitting a form with the data required for the transaction
2. The service provider decides that this transaction requires the end-user's signature
3. The service provider compose a document (text) with the essential data of the transaction and send it back to the user for signing
4. The user is reading and confirming the transaction by sending it for signing to the mSignature Service
5. The mSignature Service returns an ID of the signed document and the end-user sends it back to the service provider
6. The service provider is issuing a request for the signed document, based on the ID, to the mSignature Service: the request is signed with the service provider's signature so that the mSignature Service will agree to send him the signed document; the request from the service must arrive in a certain time interval (timeout interval) in order for the mSignature Service to satisfy it
7. The service provider validates both the end-user's signature and the content of the document: if everything match it will send a confirmation to the end-user

The process can be simplified by sending direct the signature back to the service provider instead of an ID, if the traffic of such a considerable amount of data in a request is acceptable and possible with the existent infrastructure.

3.3.2 Service provider authentication

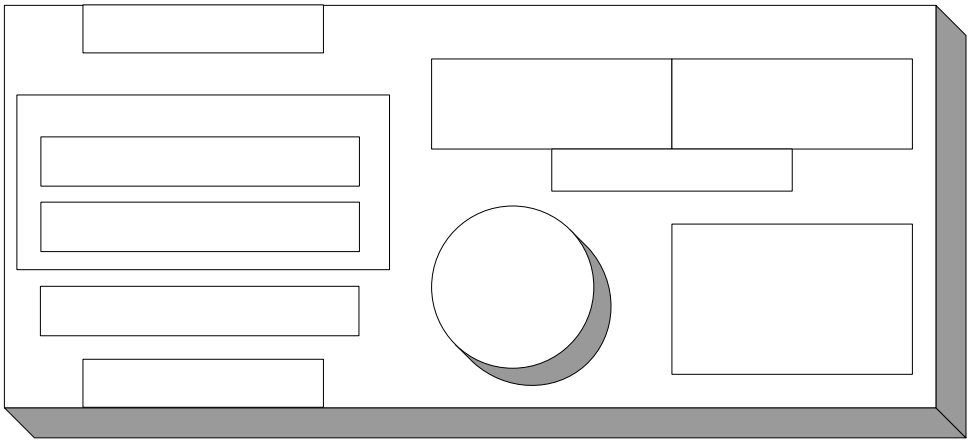
One problem the arises in the Internet world is the impersonation of service providers by fraudulent individuals/organizations attempting to find out user names, passwords, credit card numbers and other personal data that an end-user is sharing with its service providers.

To avoid this kind of mishapennings mSignature Service is providing a secure entry point to the service provider application, so that the end-user won't find himself typing his user name/password to the wrong internet address. More, mSignature Service will verify the welcome page of the service provider for it's digital signature in order to be assured of the real identity of the interlocutor, in case the service provider is down and someone else is using it's IP address for deceitful impersonation.

3.4 *Modules and functionalities*

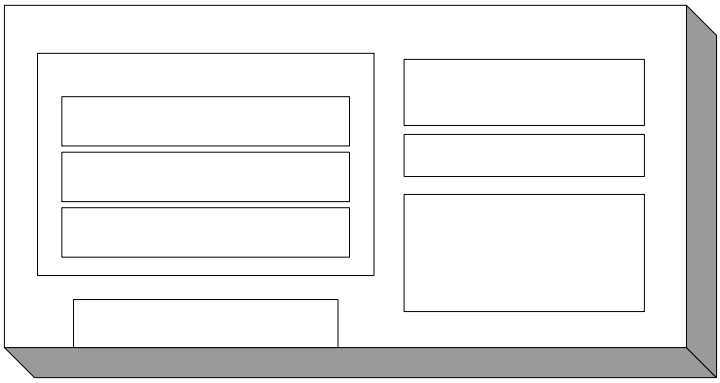
A list of the modules orchestrated by IPACRI Romania to constitute the mSignature solution is presented bellow, together with a brief list of their functionalities:

- **CA** – generation and management of digital certificates, until a real CA gets authorized
  - Certificate generation
  - Certificate management
  - Certificate revocation list
- **mSignature Service** – will digitally sign data emerging from end-user and will authenticate the service provider to the end-user
  - End-user management – user registration, digital certification upload, transaction lists, user options, other attributes, service subscriptions and preferences
  - Service provider management – service registration, digital certification upload, transaction lists, timeout interval, service preferences, other attributes
  - Operator gateway link – data packs are received from the gateway accompanied by an ID that identifies the end-user
  - Stealth mode – the connection to the internet is a one-way one: part of the Service receives commands only from the gateway
  - Data routing – in order to authenticate the service provider it must route its welcome page
  - End-user data signing – at the request of the service provider the end-user call the mSignature Service for data signing
  - Service authentication – the end-user must call the service provider through a special page provided by mSignature Service: this page will list all the services the end-user subscribed to, it will load the welcome page of the service, it will authenticate it than and leave the end-user in direct connection with the service provider; if the welcome page is not digitally signed by the service provider it will notify the end-user in consequence
  - Data encryption and decryption – if required, the mSignature Service can be used as a encryption router: sensitive data can be encrypted on sender side with the public key of the recipient to ensure that only him can decrypt and access the data
  - Signed transactions log
  - Administration and configuration
  - Statistics etc.



Digital Signature Gateway – a gateway that will process all aspects related to the digital signatures for the application

- Data routing – data must be routed through DS Proxy
- End-user management – certificates related aspects of the user management
- Web pages signing – pages must be signed for the end-user
- Signature validation – signed request incoming from the end-user are authenticated
- Data encryption and decryption – sensitive data can be encrypted on sender side with the public key of the recipient to ensure that only him can decrypt and access the data;
- Open mechanism for integration with the legacy application
- Samples



All the functionality of the DS Gateway can be also provided to the Service provider as a set of components/libraries and patterns that will allow them to develop/modify their applications for native integration with the mSignature solution.

Digital Signa

Routing for core activities

Web pages signing

3.5 *Security and feasibility considerations*

3.5.1 Security levels

Based on the choice of the End-user and/or Service provider, several levels of security can be achieved using mSignature solution:

- End-user to Service provider Requests/Data
  - Authentication and validation
    - Normal, blank delivery
    - Data signed by the operator, with or without timestamp
    - Data signed by the end-user, with or without timestamp
  - Privacy
    - No special privacy
    - SSL between device and mSignature Service and between mSignature Service and mSignature Gateway
    - Data further encrypted with the public key of the Service provider, so that only him can decrypt it
- Service provider to End-user Web pages
  - Authentication and validation
    - Normal, blank delivery
    - Pages signed by the Service provider
  - Privacy
    - No special privacy
    - SSL between mSignature Service and mSignature Gateway and between device and mSignature Service
    - Data further encrypted with the public key of the end-user, so that only mSignature Service can decrypt it and pass it to the device

End-user's digital certificate can be retrieved in two ways, based on end-user's choice:

- The end-user provides the key every time when the certificate is required (data signing or data decryption)
- The key is kept by the Proxy in order to minimize the amount of data required from the end-user

3.5.2 Digital certificates encryption

The encryption mechanism used for the local storage of the digital certificates will be based on a string password of minimum 6 characters. This may seem like a quite week encryption, so we are using an enhanced SHA algorithm with a 20 bytes digest and MD5 with 16 bytes digest, using at input the password and a bits string (seed) stored together with the certificate. The key actually used for encryption will be a byte string of arbitrary dimension as follows: A (0) = seed; A (i) = MD5 (password +A (I-1)), I>0.

The output byte string = SHA (password + A (1)) + (each of 20 bytes)
SHA (password + A (2)) +
……..

The concatenation continues in order to obtain the required length. Based on the resulted byte string the encryption system is enhanced with the generation and application of a random permutation.

A similar powerful encryption (anyway better than the usual SSL) can be used to further enhance the privacy of the communication between DS Proxy and DS Gateway.

3.5.3 Other considerations

- Both the Security and the Identification between the mobile device and the operator's Gateway is to be provided by the latter.
- The Proxy is physically located near the Gateway and directly connected to it. The Proxy only receives commands from the line that links it to the Gateway, being in stealth mode towards the Internet.
- The use of the correct certificate for a certain end-user is insured both through the operator package identification and through the key provided by the end-user at the signing moment.
- The digital certificate is stored by the Proxy, but encrypted; the encryption key is not stored and it is only known by the user.
- The solution is provided by IPACRI, by it is operated and hosted by the operator; none of them can't create any prejudice (neither through traffic monitoring or through abusive use of the certificates) without the agreement of the other; even in this case the certificates are stored encrypted with unknown keys and can not be compromised except the case when the keys have been found.
- The connection from the Proxy towards the outside environment is made through SSL.
- The proxy can authenticate the service provider to the end-user based on its signature.
- The proxy can sign the end-users' unsigned requests using a generic certificate that guarantees to the provider that the request comes indeed from a device managed by the specified operator; if the parties agree there is the possibility to provide even the used phone number or another identifier.
- The data sent by the end-user to the service provider can be encrypted using the latter's public key, so that only him will be able to access it
- There are a few minor changes needed from the service provided; they refer to program minor changes that shall allow the Proxy message routing when needed; if this is not possible or acceptable for the provider IPACRI is prepared with a Router-type solution for dealing with aspects related to electronic signing in applications black box type: this Router may be furnished under code format for the providers that intend to keep total control over the application

3.6 *Comments vis-à-vis the Romanian law for digital signature*

- Art.4 p.4 defines the attributes of the "extended electronic signature"

  a) *It is related only to the signer* - assured by the CA through the digital certificate issued to the end-user
  b) *Insures the signer identification* - assured by the CA through the digital certificate issued to the end-user
  c) *It is created through means controlled exclusively by the signer* - the end-user is the only one that is able to launch the signing through the delivery of the certificate's key ; the fact that a third party can sign on behalf of another one is confirmed by the law as bellow;
  d) *Is related to the information in electronic format, to which it compares and every subsequent modification of those is easy to identify* - provided by the use of the hash algorithm SHA-1, 160 bit algorithm, developed by NSA and NIST.

- Art.4 p.5 clearly mentions the possibility that is signing can be made by a third party (signer) in another person's name: "signer represents a person that posses a tool capable of creating a digital signature and that acts on his own behalf or as a representative of a third party.

- Art.4 p.8 defines the conditions that need to be accomplished by a "secure device of electronic signature creation".

  a) *The signature creation data, used for its generation, appears only once and the confidentiality of data may be insured* - the signature is created based on the private key attached to the certificate, which is secrete and extremely hard to counterfeit; the private key shall be stored in encrypted form; the private key does not appear in the signature; the signature shall be checked using the public key;
  b) *The signature creation data, used for its generation may not be deduced; the encryption system is based on an asymmetrical system public key* - private key RSA, min.1024 bits; the private key is not accessible and it's very hard to compromise;
  c) *The signature creation data must be protected against falsification through all available (at the moment of its generation) technical resources* - guaranteed through the hash algorithm and through encryption; DSA shall be used for signatures
  d) *The signature creation data can be protected effectively by the signer against the use of those by unauthorized persons* - the only one that has access to the database is the operator, but in the database the certificates are also stored cryptic with a key not accessible to the operator.
  e) *Not to modify the data in electronic format that need to be signed and not to hinder their being presented to the signer before the end of the signing process* - the data are always viewed by the end-user before signing; the signing method guarantees the integrity of the data.

4 Future Directions

4.1 *Technical*

Subsequent to the implementation of the mSignature solution, IPACRI Romania will progressively concentrate on the privacy issues of the present solution by approaching the two problems that can raise an issue with part of the customers:

- The digital certificates are stored at the Proxy – their security will be further enhanced and even better mechanism to prevent the access without the user's acceptance will by implemented
- A minimal intrusion in the data flow between the two parties is required – solutions to dwindle this intrusion will be devised.

In the first phase the development will concentrate on enhancing the Proxy based solution.

In the future, the new capabilities embedded in the wireless devices or the added functionality of the browser hosted by them will allow the development of device-based signatures and signature validation, but those developments are not expected to arise in the foreseeable future, anyway not in the following 18 months. At that moment IPACRI will be ready to deploy new solutions based either on MME's functionality, or SAT or BREW development.

4.2 *Business*

M-banking will become an alternate distribution channel for retail banking. E-signature enabled m-banking will allow executives to approve payments while being out of the office, in the field, far from the bank's location.

M-commerce will start to gain ground as the legislative framework will provide a safer environment and the consumers will discover the convenience of real, mobile, fast Internet.

The above tendencies will be incorporated in the next generation m-payment solutions that will allow consumers to pay by using the phone in conjunction with a bank account and/or a credit/debit card. Cross party agreements (bank-Telemobil-consumer) will even enable consumers to buy on credit. The prospective establishment of a Credit Information Bureau will contribute to an unprecedented expansion of credit.

The speed will soon increase at unprecedented levels: Qualcomm already posses the next level CDMA that will allow data transfer at 2.4 Mb/s. We will soon see a new generation of mobile devices designed to support applications that will run at these speeds, with an increased processing power, requiring larger screens and more memory. Qualcomm is preparing the future by launching BREW platform for developing applications that will use the capabilities of the new technology.

IPACRI Romania has recognized the potential released by the first 3rd generation mobile operator, Telemobil and has embarked to m-World, the future of Internet and e-commerce.

5 Conclusions

IPACRI Romania's solution is ready to accommodate the requirements for secure exchange of content over wireless network, being compliant with most of the requirements of all the parties involved and with the existent legal framework.

The concept is going to prove useful for m-commerce (not only m-banking applications) and any other communications from the mobile phones that require high-level safety.

As known, there are no digital certificate issuers already in business, in Romania. We are looking forward to see at least a Romanian operator and several International e-signature providers starting to operate during this year. However, Telemobil and the client can agree on an internal digital signature provided by any of the two.

The proposed architecture does have some minor flaws that permit IPACRI Romania and the wireless communication operator, in the very low probability of acting together with the intent to compromise the solution, to observe some of the transaction data exchanged between the parties or to manipulate maliciously the digital certificates. In this respect, we still assume that the prominence of a wireless operator (the host and the operator of the solution) coupled with the prestige of an established software house like IPACRI (the developer of the solution) constitute enough a guarantee for the acceptance of such a solution.