

MOBILE PAYMENTS – DESIGN OF NEW TERMINAL

¹Zdenko Mezgec, ¹Andrej Medved, ¹Amor Chowdhury, ²Rajko Svečko

¹Ultra d.o.o., Research centre, Maribor, Slovenia

²University of Maribor, Faculty of Electrical Engineering and Computer Science, Maribor, Slovenia

Key words: Mobile payment, GSM, Voice, Terminal

Abstract: Mobile phones and mobile access to internet are creating new space for challenges and ideas in companies business. And today's electronic revolution in electronic payments is promising even more mobile involvements in money. Mobile phones are far from just a device for communication with other people. They are overtaking functionalities of camera, personal computers, media players and others devices. But most of all mobile phones are also used for mobile payments. Because of great inquiry for mobile payments, different technologies were developed. Company named Ultra d.o.o. has developed new mobile transaction system. Data transmission is transmitted over the speech channel of different mobile communication systems such as GSM, CDMA and UMTS. Ultra d.o.o. has already obtained two international patents for this type of transmission. The basis of this mobile transaction system is voice-coded data transmission between the transaction authorization processing centre and the terminal.

The system is generally designed for two types of terminals; the mPOS and aPOS, which are meant for different applications. The terminal is a device which works similarly like a POS terminals.

In today's world there are increasing demands for mobile transaction systems that would enable a palette of services, portable, light, small, ergonomically designed and enabling different transaction technologies, all in one device. Demands like that have brought to new terminal concept, which we describe in this article. The main aim of the article is to present the transfer procedure form idea to practical realization and inside of this the technical evolution of electronic device-terminal which is a crucial part of the invented transaction system.

Mobilno plačevanje – razvoj sodobnega terminala

Ključne besede: Mobilno plačevanje, GSM, POS, terminal

Izveček: Mobilni telefon postaja nepogrešljiv del vsakdanjih opravil. V povezavi z drugimi tehnologijami prevzema tudi funkcionalnosti drugih naprav, na primer fotoaparata, dlančnika, mp3 predvajalnika... Vse močnejši trend mobilnih telefonov postaja uporaba mobilnega telefona za plačevanje. S porastom zanimanja za mobilna plačevanja so se in se še vedno razvijajo najrazličnejše tehnologije, ki omogočajo hitro, enostavno in prijazno mobilno plačevanje.

Podjetje Ultra d.o.o. je razvila lastno tehnologijo mobilnega plačevanja, ki temelji na osnovi prenosa zvokovno moduliranih podatkov po govornem kanalu različnih mobilnih omrežij. Glede na različne plačilne storitve in uporabo, sta se razvila dva tipa terminalov in sicer aPOS ter mPOS.

V sodobnem času se kažejo čedalje večje zahteve po POS napravah, ki bi omogočale široko paleto najrazličnejših servisnih storitev. Zraven tega morajo biti še prenosne, lahke, majhne, čim dalj časa avtonomne, ergonomsko oblikovane, hkrati pa bi omogočale uporabo različnih tehnologij plačevanja. Takšne zahteve so pripeljale do novega razvoja terminala, ki ga opisujemo v tem članku.

1. Introduction

Mobile businesses and mobile internet access are creating new challenges for business operations in all lines of business. The present-day electronic revolution in electronic payments is promising an enhanced role of electronic money in modern life. Mobile phones have long ago stopped being a mere communication device, but are now also assuming functions of cameras, computers, palms, media players etc. For an increasing number of users they also represent a mean of payment. Due to an increasing interest in mobile payments different technologies (SMS, GPRS, RFID etc.) providing such services have been developed.

The company Ultra d.o.o. has developed its own technology based on data transmission through a speech channel of different mobile networks, such as GSM, CDMA and UMTS /1/, /2/, /3/. The abovementioned mean of data transmission is enabled by a system with two international patents.



Fig 1: The basic principle of system operation.

The advantages of the mentioned payment-technology system against others make further developing sensible. These advantages are the following:

- Passive communication terminal: all transmitted and received data travels through a speech channel of the user's mobile phone.
- The use of technology is independent of the mobile phone standard or mobile network. All mobile phones include the primary function of transmitting and receiving speech.

Contemporaneity shows an increasing demand for POS devices that would enable a wide range of different services, such as payments, deposits into pre-subscriber accounts, bonus-points program etc. In addition they should be portable, light, small, autonomous for as long as possible and ergonomically designed. Support of other payment technologies is also needed to compete with existing terminals, so that a single terminal would enable different payment technologies, which is friendlier for the users as well as merchants, who already have too many different terminals at the pay points, which causes a certain degree of confusion. Such demands resulted in an advanced terminal, described in this article.

The article first presents the development of an advanced terminal, and development of terminal's external design, development of printed circuit and development of testing technologies are presented respectively. In the following chapter the overall functionality and the structure of the terminal are described. Applied wireless communication devices are presented next. Special chapters are devoted to terminal protection as well as data transmission through mobile network's speech channel. As final comes a chapter on the concept of the software part, which unites the aforementioned parts of the terminal.

2. Development of the terminal

2.1 The development of the external design

External design was developed gradually in CAD (computer-aided design) software environment /5/, /6/. The terminal has to be small, portable and ergonomically designed. It also has to take into consideration many other factors. The basic functionality of the terminal are mobile phone payments. Because of that the acoustic set has to be as adapted as possible for best data transmission between individual microphones and speakers. The design is also defined by different card slots, connectors for outside world connections and the size of the screen, keyboard, printer, speaker, microphones and other major components of printed circuit. Fig. 2 shows successive modifications of the external design with regard to the mentioned demands.

Further development of the terminal's design takes into consideration additional modifications that appear after the first tests of the acoustic set of the new terminal. Acoustics test is done on the casing, made with stereolithography technology. Extra deviations due to different plastic matter and accordingly different acoustic characteristic are taken into consideration. At the same time an additional layer of soft rubber is applied on the top casing, to prevent mobile phones from sliding of the terminal. The development of printed circuit was parallel to the development of the external design of the terminal. Because of that the external design was modified simultaneously according to smaller or larger modifications of the printed circuit. Fig. 3

shows the final external design of the terminal on a dock station, which is often used with the terminal.

2.2 Development of printed circuit

The development of printed circuit was parallel to the development of the external design of the terminal. Planning of printed circuit was done in three software environments. Planning of the circuit scheme was done in one software environment, planning of PCB (Printed Circuit Board) in another, and three-dimensional planning of the circuit and all electronic components was done in the third CAD software environment /5/, /6/, /7/. All three software environments are interconnected, so that for example a change of position of one of the electronic components in software environment for PCB composition reflects in the change of position in CAD software environment. This way the entire development is done in software environments and there is no need to create intermediary printed circuits to examine compatibility with the terminal's casing.

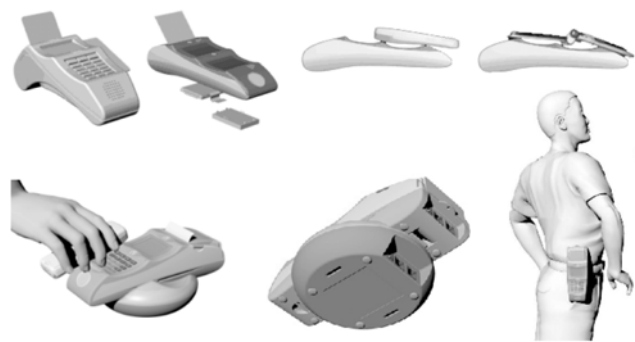


Fig. 2: Gradual development of the external design of the terminal.



Fig. 3: The final design of the terminal with dock station

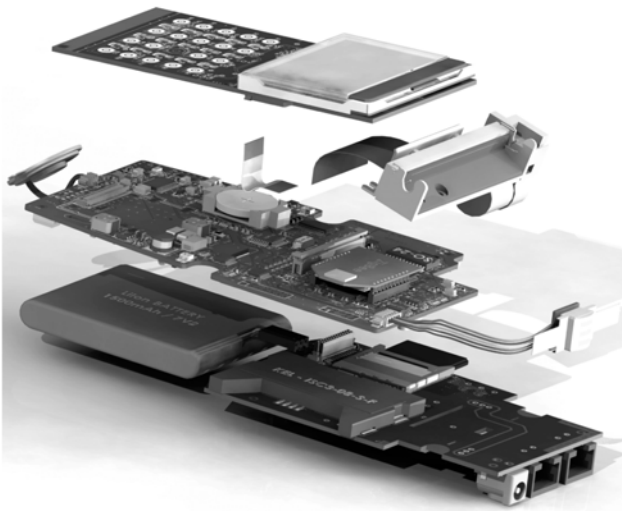


Fig. 4: The electronic part and the printed circuit of the terminal.

The electronic part of the terminal is roughly divided into 6 separate parts as follows (Fig. 4):

- Primary printed circuit includes:
 - central processing unit,
 - external memory units,
 - power management circuit.
- Secondary printed circuit includes:
 - screen and a keyboard
 - an antenna and RFID communication circuit,
 - a codec for collecting and producing sound.
- Lower printed circuit includes:
 - power connector
 - RJ45 connectors
 - SD connector
 - smart card connector, etc.
- Magnetic head for cards with a magnetic record,
- Printer
- Battery
- Speaker and microphones

With three-dimensional planning of printed circuit every used component needs to be transferred into CAD software environment. For some components manufacturers provide three-dimensional information, for the rest we provided them ourselves.

A part of creating printed circuit is testing PCB [4]. Considering that all printed circuits were planned also in CAD software environment we could also use the latter for easier planning of the testing device for PCB test. The mentioned choice of planning includes several advantages against standard methods of planning. One of them is also simpler preparing of test needles holes. With such planning a testing device can be created even before the first prototype of the printed circuit is made. By projecting printed circuits or marked testing points onto the lower testing board documentation on exact measures of the drilled

openings as well as on other important information, such as end-height of individual components and suchlike can be sent to the manufacturer of testing devices.

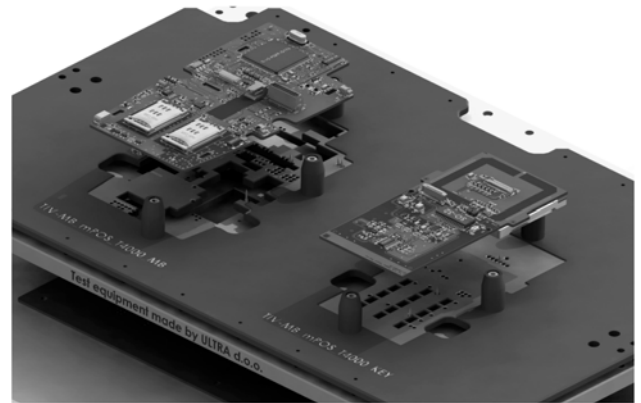


Fig. 5: A testing device for terminal printed circuits

3. Functionality and the structure of the terminal

The basic functionality of the terminal is performing different types of transactions. These can be carried out in different ways, since the terminal supports different technologies of user-identification (RFID tag, magnetic-stripe card, smart card and mobile phone's MSISDN) as well as different ways of communication with the centre like data transmission through a speech channel of a mobile network, GPRS, Ethernet wire technology, ZigBee. The choice of individual communication channel depends on the price of data transmission, the speed of data transmission and the location of the use of the terminal.

Besides the basic functionality, the terminal also provides others. We will only mention a few more important ones. The terminal enables distance maintenance or replacement of the software part of the terminal, display of different transaction extracts (reports, account, duplicate) on the screen and on paper via printer, portability of the terminal – battery and recharging option, corresponding display and a simple user-interface, transmitting or producing voice instructions, protection of the terminal against unwanted intrusion. For the sake of all the mentioned functionalities the terminal is constructed in several parts/sets:

- digital signal processor (FLASH and RAM)
- memory components (EEPROM, SD card etc.)
- circuit for protection against unwanted invasion
- power management circuit,
- battery
- connectors,
- keyboard,
- screen,
- printer,
- wireless technologies (RFID, GPRS, ZigBee),

- RTC (real time clock),
- smart card for ECC cryptography.

Fig. 6 and fig. 7 show individual sets and the basic structure of the terminal.

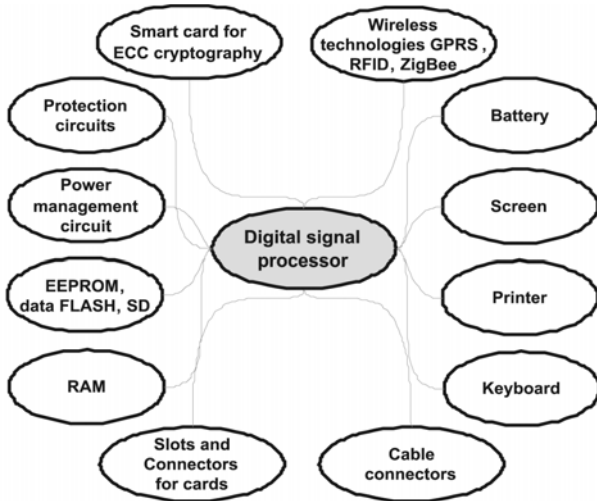


Fig. 6: The important sets of the terminal.

3.1 Central processing and external memory units

The central processor of the terminal is a 32-bit DSP (digital signal processor) TMS320F2812 made by company Texas Instruments, which has integrated peripheral buses. These directly support SPI, SCI, AD, PWM, QEP, McBSP CAN etc. The mentioned DSP supports 16x16 and 32x32 MAC (Multiply and Accumulate) operations and 16x16 double MAC operations. The core of the DSP runs with a frequency of 150 MHz and achieves the capacity of 150 MIPS (Million Instructions per Second). All the above-mentioned characteristics are necessary for real-time processing of different operations performed by the terminal:

- FFT (Fast Fourier Transformation) and IFFT (Inverse FFT),
- filtering of individual carrier frequencies,
- encryption and decryption of data,
- BEC (Backward Error Correction),
- FEC (Forward Error Correction),
- GUI,
-

TMS320F2812 digital signal processor has an integrated internal FLASH and RAM for storing and processing program code and data. The following memory units that serve different purposes are connected directly to DSP: external static RAM, serial FLASH, EEPROM, additional alternative SD card and an interface for smart cards.

A version of PCB is saved in EEPROM, which enables easier service as well as proper functioning of one pro-

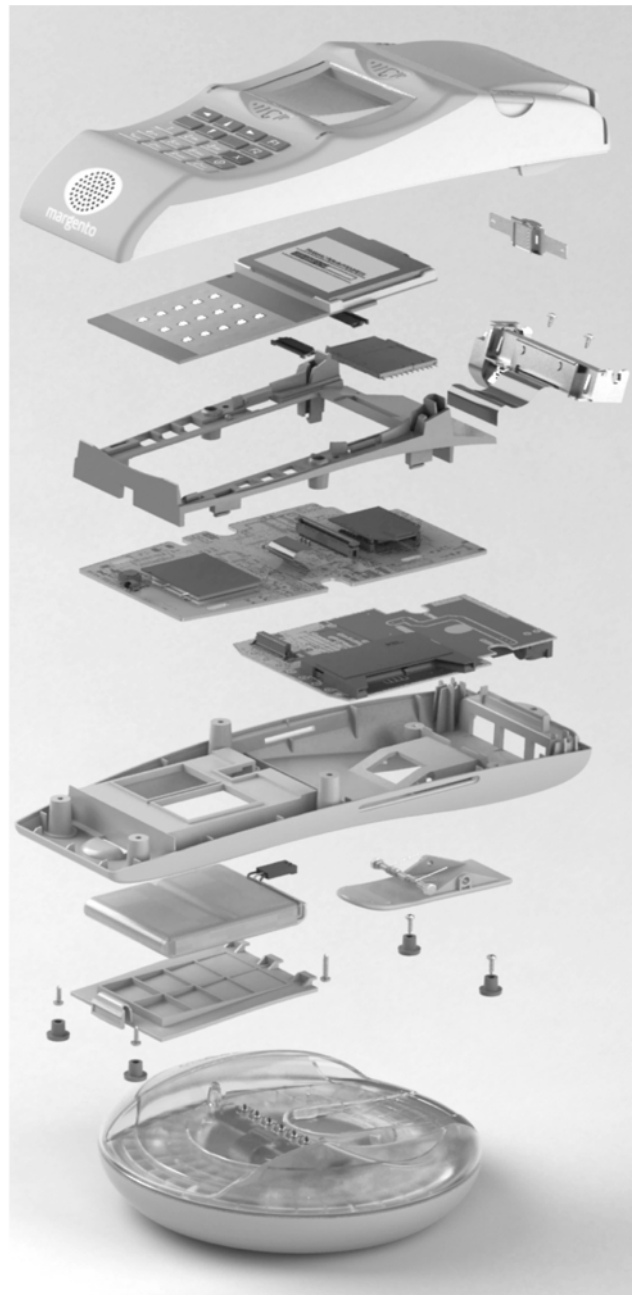


Fig. 7: The structure of the terminal.

gram code on different PCBs. Parameters which determine the functioning of the program code as well as storage of data needed by the terminal when restarted are also saved in EEPROM.

Internal and external RAM are used for debugging in the development environment, as well as for storing data and performing individual program algorithms that have to be performed faster (FFT, correlations, filtering etc. using faster internal RAM).

Graphic data records, used for animations, text extracts, screen logotypes and thermal printer logotypes; as well as sound data records for proper signalization are stored in external serial FLASH. The latter is also used for storing transaction data and partial storing of the program code etc.

SD cards are used for storing additional advertising data such as logotypes, animations and larger sound records. At the same time the same input slot is also used for upgrading the terminal with a program card that holds the program code.

Smart card interface has four different functionalities. The first functionality is supporting credit cards for user identification and performing payment transactions. The second functionality is the use of merchant-identification cards. The third functionality is saving sensitive data onto protected cards. The fourth functionality is performed on a separate parallel port intended for alternative use of smart cards for storing cryptographic keys and performing corresponding cryptographic algorithms.

4. Wireless communication

Nowadays many devices use wireless communication, which primarily provides portability of the device. The following wireless communications are used with the terminal:

- ZIGBEE,
- RFID (Radio Frequency Identification),
- GPRS (General Packet Radio Service) and
- transmission of data through a speech channel of a mobile network.

The terminal uses ZigBee for wireless communication between the terminal and the dock station. The mentioned functionality is used only when the dock station is connected to ethernet network or the cash point directly. In this case ZigBee becomes a bridge, that enables indirect connection of the terminal to Ethernet network or the cash point.

RFID wireless communication is used for two different functionalities. Primarily it enables registration before the use of the terminal, which limits access to the terminal only to authorized persons or cards. At the same time the terminal and RFID also enable mobile payments through NFC (Near Field Communication) standard. With this the terminal enables 4 different means of payments, that is:

- smart cards,
- cards with a magnetic record,
- NFC and
- mobile payments with transmission of data through a speech channel of a mobile network.

In individual countries transmission of data through GPRS channel is relatively inexpensive. Apart from GPRS modem the terminal only needs a valid SIM card of a mobile operator. In this case mobile payments are done so that user identification is sent through a voice channel to the terminal, and all other data is sent through GPRS channel. Such transactions are faster and more robust, and the terminal also has the possibility to upgrade larger parts of software, which consequently means easier maintenance of the terminal.

4.1 Communication through a voice channel of a mobile network.

Transmission of data through the voice channel of a mobile network is the most important wireless communication of the terminal. Advantages against others have already been listed in the introductory chapter. Several different problems that prevent high speed of data transmission arise with this method of data transmission. Because of this the terminal includes different systems for correcting and detecting data as well as modified modulations for more robust data transmissions. Fig. 8 shows individual systems in charge of data transmission between the terminal and the centre. Among them is also encrypting and decrypting of data, based on ECC cryptography.

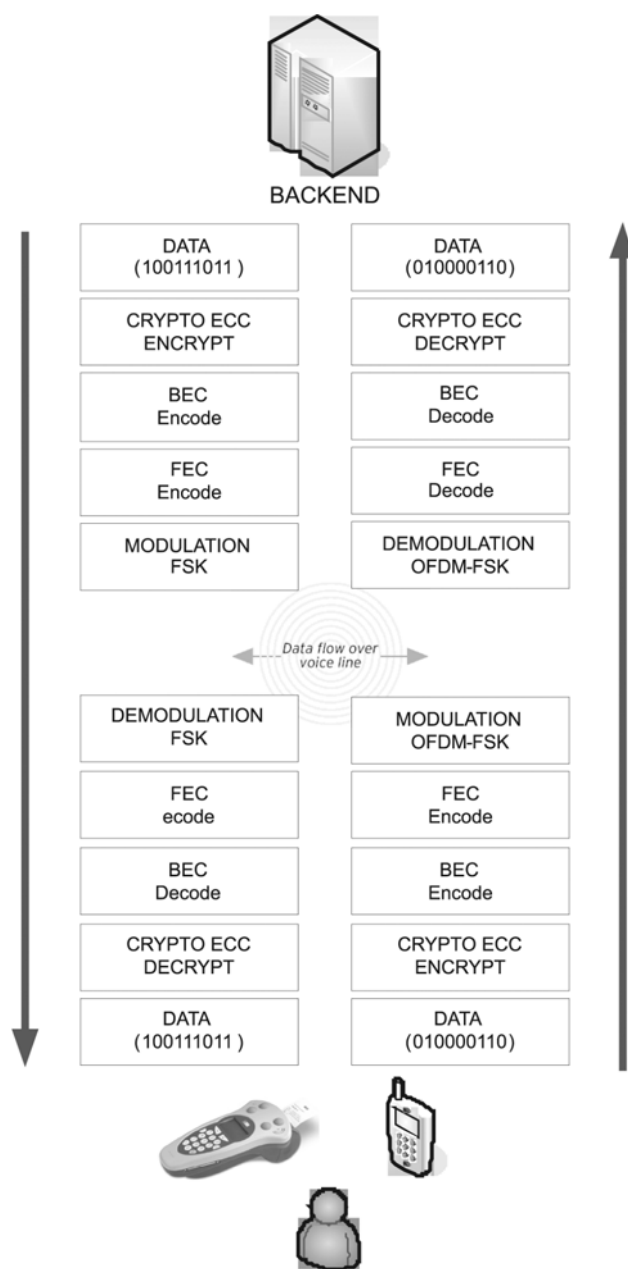


Fig. 8: Provision of robustness of data transmission with different systems or algorithms.

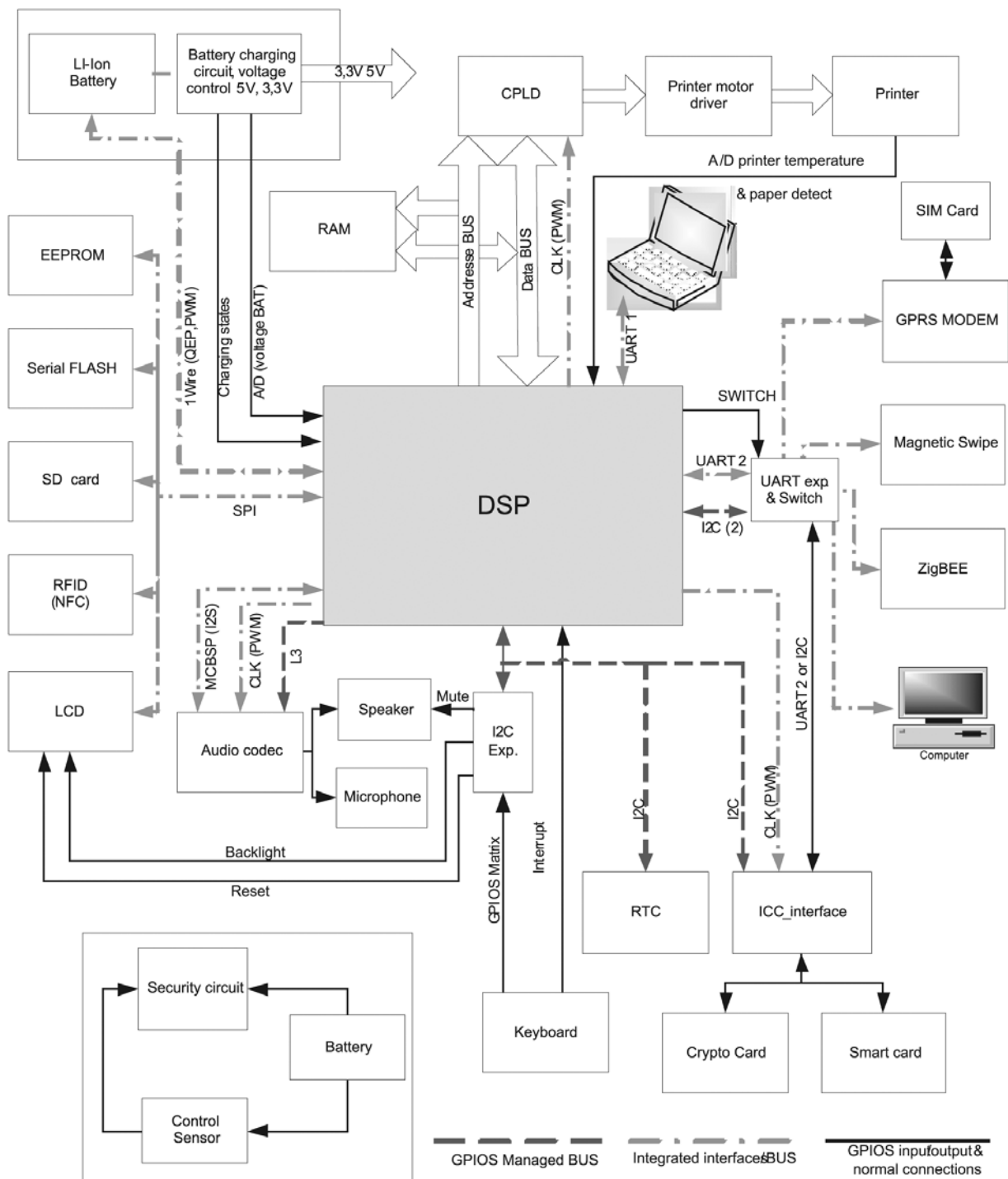


Fig. 9: Block diagram of the printed circuit of the terminal

Center and terminal are communicating in full-duplex mode. Terminal has to simultaneously in real-time perform demodulation and modulation, FEC (forward error correction) decoding and coding, BEC (backward error correction) decoding and coding and ECC encrypting and decrypting of data. For modulations and demodulations adaptive and robust techniques have been developed especially designed for voice coded transmission over speech channels in mobile networks. Those are based on modified OFDM techniques, pilot signals, chirp signals and different advanced channel analysis.

5. Terminal protection

The primary function of the terminal is performing money transactions. Because of this a high level of protection is necessary. Besides the protection of data transmission, protection against unauthorized physical intrusion to the terminal is needed. Protection circuit runs in connection to separate power supply and protection sensors. The mentioned protection must ensure that:

- it is not possible to intercept data running between the keyboard and the processor,

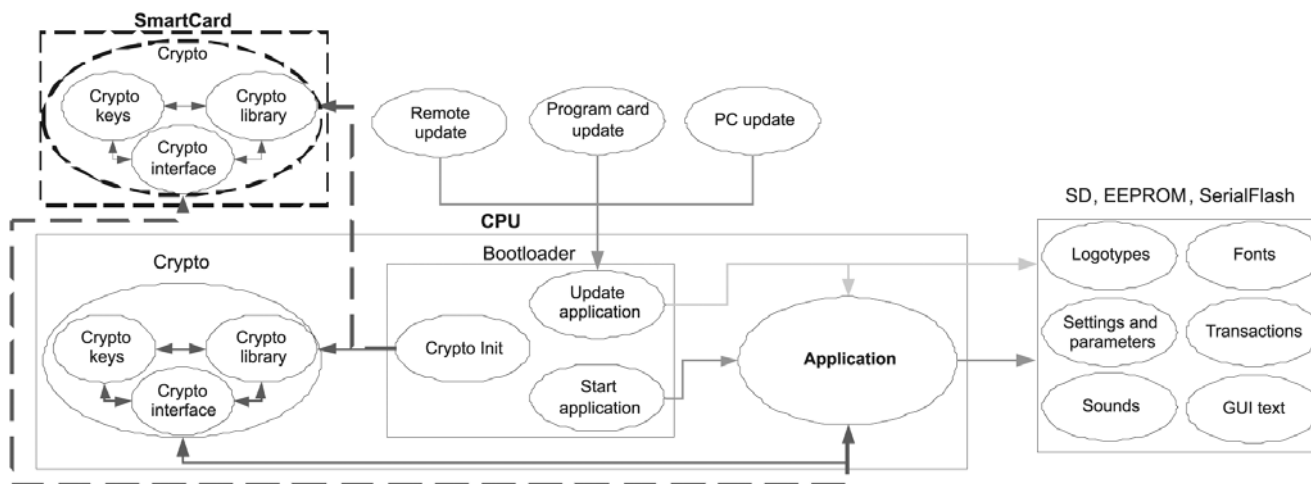


Fig. 10: Block diagram of the software part of the terminal

- it is not possible to intercept data running between the cards and the processor, and
- it detects and promptly reacts in case an unauthorized person tries to open the terminal.

Additional protection of data is provided with a 128-bit key that locks the processor, and at the same time especially sensitive data is saved onto an extra crypto smart card.

6. Software part

Fig. 10 shows a block diagram of the software part of the terminal, which is roughly divided into 4 parts: Bootloader, cryptography, main application and additional data.

Bootloader performs several tasks. At startup it first checks if a program card containing a new application is inserted into the terminal. In this case it updates the application and data in external memory units. In a similar way the terminal can be updated through a maintenance call or directly via PC.

Maintenance call enables distance updating of the application, which means that individual parts or the whole application is sent from the centre to the terminal through a channel that is used by the terminal for communication with the centre at the time. The next task of the bootloader is initialization of cryptography and afterwards startup of the main application. The terminal uses cryptography of elliptic curves ECC that is based on public and private keys / 8/. The cryptography is made up of crypto keys, crypto library and a crypto interface. It can all be done on a locked DSP or on a smart card. The latter has more advantages, among others also easier service of the terminal and disburdening of the DSP.

The main application is the core of the terminal and the largest software part since it connects all the presented components and performs different algorithms in charge of GUI, drivers, protocol and communication level of trans-

actions, reports, wireless communication, saving and reading the data and several other important tasks. All these algorithms are communicating via well known services for synchronization (semaphores, mailboxes, queues etc.), scheduling (multitasking, periodical functions, interrupt manager) and other system services. s communication, storinted components safter that startup of the main application.g cryptgraphig algorithms

7. Conclusion

The presented article describes the development and the implementation of a modern terminal. The terminal provides a wide range of different services, enabling different methods of mobile payments as well as other functionalities that distinguish the terminal in many aspects. The terminal has a unique design that corresponds to the primary functionality, i.e. mobile payments with transmission of data through a speech channel of a mobile network. At the same time the presented terminal is an autonomous and small device that includes a high level of protection against intrusion to the terminal. Communication between the terminal and the centre runs through different wireless and wire technologies, which additionally enables easier integration of the terminal into the existing systems or environments. The terminal is constructed so that printed circuit can be added or modified without changing the external design of the terminal. For further development of the terminal a replacement of the core processing unit with a stronger one is foreseen, and at the same time the development will be in line with compatibility with the existing wire technologies (integration of Ethernet module etc.).

8. Literature

- /1/ Ultra M-Pay worldwide patent WO0233669, "System for payment data exchange and payment terminal device used therein", 2002
- /2/ Ultra M-Pay worldwide patent WO03088165, "Payment terminal device for payment data exchange", 2003
- /3/ Z. Mezgec, A. Chowdhury, R. Svečko, "Transmitting data through the GSM mobile phone voice channel", IWSSIP Budapest, Hungary. 2006
- /4/ Z. Mezgec, S. Goličnik, A. Medved, A. Chowdhury, "Naprava za avtomatsko testiranje funkcionalnosti M-Pay terminala", Konferenca AIG'07, Maribor, 2007.
- /5/ CAD/CAM/CAE Pro/ENGINEER Solutions, <http://www.proengineer.com/>
- /6/ 3D Mechanical Design and 3D CAD Software, <http://www.solidworks.com/>
- /7/ P-CAD, Specialized design tool for PCB layout, <http://www.pcad.com/>
- /8/ G. Agnew, R. Mullin and S. Vanstone, "An implementation of elliptic curve cryptosystems over F2155", IEEE Journal on Selected Areas in Communications, (1993), 804-813

*Zdenko Mezgec, univ. dipl. inž. el.,
 Andrej Medved, univ. dipl. inž. el.,
 dr. Amor Chowdhury,
 Ultra d.o.o., Razvojni center,
 Gosposvetska 84, 2000 Maribor, Slovenia
 E-mail: zdenko.mezgec@ultra.si*

*prof. dr. Rajko Svečko
 Inštitut za avtomatiko,
 Laboratorij za sisteme in vodenje,
 Fakulteta za elektrotehniko, računalništvo in
 informatiko, Smetanova 17, 2000 Maribor, Slovenia
 E-mail: rajko.svecko@uni-mb.si*

Prispelo (Arrived): 02.10.2007 Sprejeto (Accepted): 28.03.2008