Contents

1. About Payment Technologies Holding Company ...................................................................................... 3
2. Clients ......................................................................................................................................................... 4
3. Check-In-Phone .......................................................................................................................................... 5
4. Check-In-Phone technology ....................................................................................................................... 6
5. Check-In-Phone Architecture residing at mobile phones ........................................................................... 8
6. Server architecture of Check-In-Phone applied products ......................................................................... 12
7. Check-In-Phone Security .......................................................................................................................... 14
8. Integration with the Client’s Call-centre. Main issues ............................................................................. 24
9. One-time passwords for Internet-banking checking ................................................................................. 28
10. Check-In-Phone: transactions with authentication made with banking cards ........................................ 31
11. Check-In-Phone: EMV-card and reader for OTP generation on CAP algorithm ..................................... 32
12. Check-In-Phone: money transfer and cash withdrawal in ATM or branch without the card ................ 34
13. Check-In-Phone services configuration ................................................................................................ 36
14. Support and compatibility ..................................................................................................................... 36
15. Main priorities ....................................................................................................................................... 43
16. Persons ................................................................................................................................................... 44
17. Banking details ........................................................................................................................................ 45
18. The services components ....................................................................................................................... 46
19. The licenses procured with the solutions ............................................................................................... 47
20. Software ................................................................................................................................................. 48
1. About Payment Technologies Holding Company

Payment Technologies Company began its activities in 2000 as a daughter enterprise within the Finance-Industrial Federation Holding. Payment Technologies Company’s (PT Company) core team consists of STB Card Development Department that also was the daughter structure of the Finance-Industrial Federation Holding.

The PT Holding’s staff has a long-standing unique experience in the Russian Federation in designing, building, implementing and maintaining real-time computer systems applying to the cashless settlement and identification systems based on chip and magnetic stripe cards, mobile solutions.

PT Holding delivers technological consultancy, carries out analytical and research jobs, elaborates project, technological, normative and operational documentation, implements and supports approved real-time systems for large-scale projects of its customers.

The PT Holding staff has been actively contributing to the field of implementing of real-time systems relating to terminal equipment identification and managing. A treasure of experience have been build up by PT’s staff in the field of implementation, maintenance and developing of the computing complexes meant for realizing cashless payments systems based on cards, remote services systems.

PT Holding provides consultancy and designing of standard worldwide approved computing complexes for real-time systems, assists customers in choosing adequate technical and technological tools to achieve their production, social and commercial goals and to set up a solid technological basis for their operation activities, manages projects on a turn-key basis.

Combining deep theoretical knowledge and vast practical experience, PT Holding offers solutions of utmost efficiency on development and integration of computer systems for everyday processing activity.
2. Clients

1. SIAB Bank (2009) – first CIP product customer!
2. VISA (2009)
3. MasterCard (up to now)
5. Transcreditbank (2008)
6. Home Credit&Finance Bank
7. IBS (up to now)
8. AK Bars Bank (2003-2007)
13. AKIBANK
14. Alfa Bank
15. Russian Europay Members Association
16. Bank «1 OVK»
17. Bank «Severnaya Kazna»
18. Komneyvabank
19. Masterbank
20. NKO ORS
21. Noyabrskneftecombank
22. STB Card
23. Surgutneftegazbank
24. Transinvestbank
25. Finansbank
26. Comcor
27. Hewlet Packard
3. Check-In-Phone

Check-In-Phone – a trade mark.

Check-In-Phone – an open secure technology, providing round-the-clock delivery of services companies, employees or customers (Check-In-Phone Users) directly to their mobile phones.

Check-In-Phone – a reliable standard tool for Check-In-Phone Users authentication required by Check-In-Phone Partner for personalized services rendering based on MasterCard CAP (MMA).

Check-In-Phone – an opportunity for the company to elaborate the personal set of remote services for its customers – Check-In-Phone Users.

Check-In-Phone – a secure message exchange between the companies and Check-In-Phone Users; as well among Check-In-Phone Users themselves.

Check-In-Phone – a JAVA (MIDP 2.0 – compliant) and Windows Mobile application loaded to a mobile phone of Check-In-Phone User and providing remote access to services of different informational systems. Beginning with the 3Q2009 – Check-In-Phone iPhone program is available.
4. Check-In-Phone technology

Check-In-Phone is a technology which provides secure delivery of services (elaborated by the Customer and its partners) via mobile phones of Check-In-Phone Users or other equipment specified by the Partner.

JAVA-compliant mobile phones (version higher MIDP 2.0 (JSR 118), specified for CLDC 1.0 (JSR139) equipment), Windows Mobile devices and iPhones can be used in the Check-In-Phone system. Customer devices have to support high-speed communications like GPRS and EDGE.

Check-In-Phone Partners should bear in mind that mobile phones non-compliant with the above requirements couldn’t be used by the prospective Users.

Check-In-Phone technology provides:

- Independence from cellular carriers for Application Issuers (personal sets of remote services);
- Easy loading/deletion of new Applications elaborated by parameterization by Issuers and Users.
- Opportunity to apply different inexpensive tools for downloading of Check-In-Phone Mobile Container and Wallet: GPRS, EDGE, Bluetooth, IRDA, NFC and etc.
- Opportunity to widely apply multimedia resources embedded in a mobile phone.

A reliable and secure CAP-based authentication procedure to access services provided by Check-In-Phone Partners is used in the Check-In-Phone system. The procedure is in compliance with the MasterCard Mobile Authentication (MMA) standard.

An information system supported by the Partner that provides the User with a service as it is (f.e. remote banking, e-commerce, blocking a card on call, contacting average commissioner when traffic accident occurs, making an appointment with a doctor in voluntary insurance system and etc.) plays a key role in service rendering.
On-line interface is used for arranging interaction between the Check-In-Phone system and Partners’ information systems aimed at authentication.

Services are rendered both by means of Check-In-Phone Mobile Containers, Wallets and Applications downloaded to mobile phones and Check-In-Phone central servers, realizing (according to service – focused architecture) business logic of the access to Check-In-Phone Partners, services available for Check-In-Phone Users directly from their mobile phones. The Manager offers the Partners registered as Issuers to use the markup language of the Wallet CIPML (Check-In-Phone Mark Up Language, that is the subset of the XML language) for short and understandable description of Applications business logic and generation of the clients interface of the Application at the mobile phone.
5. Check-In-Phone Architecture residing at mobile phones

Check-In-Phone architecture running on the User’s mobile phone is described below.

Check-In-Phone Mobile Container rested on JAVA-technology embedded in a mobile phone is actually a foundation, a core, a platform where the following technologies are realized:

- Check-In-Phone Wallet that is actually the Application of Check-In-Phone Manager,
- Applications of Check-In-Phone company.

Picture. Check-In-Phone residing at a mobile phone (architecture)

Check-In-Phone Mobile Container is an application (a program for Java2ME, Windows Mobile or iPhone) which realizes different functions including CAP Token calculation (Mode 2, Mode 2 with TDS) to support different business logic of different business
applications. One of the end results of the program, a calculated CAP Token value, is used both for one-time passwords (OTP) generation and for signing the sensitive data in Check-In-Phone Applications.

Check-In-Phone Mobile Container is the first program to be downloaded to a mobile phone.

Among various Check-In-Phone Applications embedded in a mobile phone there is Check-In-Phone Wallet – the Application ranked as a special Application and realizing service functions with regard to other Applications at a mobile phone. The special position of the Wallet is that it’s downloaded to a phone for the second turn (immediately after Check-In-Phone Mobile Container downloading) and then is used for secure loading and activation of other Partners Applications at a mobile phone, including but not limiting:

- Arranging secure loading of Check-In-Phone Applications;
- Check-In-Phone Applications activation;
- Check-In-Phone Applications deletion;
- Restoring personal data of Check-In-Phone Applications;
- Arranging user-friendly client interface to interact with Check-In-Phone Applications (particularly, receiving lists of available Issuers Applications and choosing an Application for downloading to a mobile phone);
- Arranging secure channel for data transmission from Check-In-Phone Application to its Issuer;
- Managing Issuers Applications by Check-In-Phone Users, including their blocking and deletion.

Taking into account that Mobile Container and Wallet being the elements of Check-In-Phone infrastructure are not operating separately (except for some initiative operations) further when we speak about Check-In-Phone Wallet we mean Mobile Container and Wallet together, if they are not required to be mentioned separately.

Check-In-Phone Mobile Wallet is loaded to any Users mobile phone during Issuers Applications loading by Users order. One couldn’t load Issuer’s Application without Check-In-Phone Mobile Wallet has been previously loaded.
The structure of the Mobile Wallet downloaded «over» the Mobile Container and the structure of Applications are mainly the same as they realize their service functions for Check-In-Phone Users mainly in the same way.

The following data are used within Check-In-Phone Mobile Wallet:

- Data for the wallet identification
- Key data to generate signatures and encrypt data and other confidential data
- URL of Check-In-Phone authentication system
- Common variables
- CIPML code of the Mobile Wallet (its marking)
- Choice of the language used to interact with Check-In-Phone User/on default-Russia
- CAP profile.

All the above data of the Wallet are available only for Check-In-Phone Mobile Container and is not available for other Applications.

The following data is used within Check-In-Phone Application:

- Application identifier
- Key data and confidential data
- URL of Partners server registered as an Issuer
- CIPML code of the Application
- Choice of the language used to interact with Check-In-Phone User
- CAP profile.

All the above data is available only for Check-In-Phone Mobile Container and is not available from other Applications.

The confidential data of Applications is stored encrypted. The component part of the encryption key is a PIN-code entered by Check-In-Phone Applications User.
Check-In-Phone Application’s Interface for Check-In-Phone User contains navigation aids, procedures for data transceiving as well as procedures for data screening, data receiving, data inputting be the User through phone pad and means for interaction with external program units (plug-ins). Interface is built up by the markup language CIPML and defines business logic of the Application.

The menu content of Application can be amended both by Issuer of Application (Check-In-Phone Partner) and immediately by Check-In-Phone Application’s User. The menu content can be changed in User’s Private Office through Web-interface or directly from the mobile phone.

Personal data includes characteristics of the particular Application elaborated by a certain Check-In-Phone Partner registered as Issuer for the particular Check-In-Phone User.

The functions of the Application are mainly defined by business requirements.

Applications use the program code of Check-In-Phone Mobile Wallet for carrying out cryptographic procedures and other functions. Business logic and required data for Application correct running are installed together with the Application downloading to a mobile phone.

The elaborated Check-In-Phone architecture is service-oriented and it allows Check-In-Phone Partner to design and elaborate Check-In-Phone Applications by himself by means of CIPML markup language and specifications related to Check-In-Phone Application.
6. Server architecture of Check-In-Phone applied products

The main components of the CIP architecture are as follows:

- Issuers (Check-In-Phone Partners) Application running under supervision of Check-In-Phone Mobile Wallet at the Check-In-Phone User mobile phone.

- Server CIP subsystem: Authentic Gate (AG).
- Server CIP subsystem Applic Ward (AW).
- Server gateway subsystem - CIP Access Point (AP).

The Check-In-Phone AG server subsystem interacts with the Check-In-Phone Application/Wallet on the basis of HTTPS.

All incoming requests (that is, forwarded from Check-In-Phone at a mobile phone to the server Front-End subsystem) are transferred to CIP AG of the Front-Office server subsystem for processing.

CIP AG carries out all necessary procedures. For Users request processing CIP AG will communicate with information subsystem bank to CIP AP that is the Issuer of the Application.

CIP Applic Ward is assigned for realization of milestone events within the life cycle of the Check-In-Phone Application starting from the Wallet loading to Applications activation for the particular User.

Users of the certain Application (at Bank decision) are provided with web-interface to the Users Personal Offices, allowing Users to look through the personal data (f.e., card balance, mini-statement), as well as change Check-In-Phone menu at the mobile phone. Access to Web-interface is provided after the one-time password entered, OTP is generated by means of Check-In-Phone at a mobile phone. This access is realized through CIP AW.
To manage Applications, authorized persons of Check-In-Phone Partners (operators and/or administrators) are provided with the corresponding access to CIP AW through CIP AP.

The following features of the CIP system architecture should be pointed out:

- Service-oriented architecture;
- Scalability and extendibility;
- Modularity;
- Multilingual support;
- Multiple delivery protocols (GPRS, SMS, EDGE….);
- Availability of means for prompt elaboration of Applications (business scripts);
- Elaboration of Applications by means of markup language (XML, CIPML);
- Independence from cellular carriers;
- Opportunity for managing the Applications main menu and the list of offered Applications through the phone menu;
- Opportunity for managing the Applications main menu and the list of offered services through Web-interface;
- Opportunity for flexible configuring and adjusting aimed at realization of new remote services elaborated by Check-In-Phone Partners; opportunity for launching marketing and advertising programs by Partners jointly.
7. Check-In-Phone Security

Check-In-Phone technology is based on the use of the MasterCard Mobile Authentication (MMA) protocol. To realize MMA standard in Check-In-Phone, Check-In-Phone Mobile Wallets are downloaded to user mobile phones. These are the special programs (JAVA-applications or midlets for J2ME platform, version MIDP/JTWI/MSA at a mobile phone), Windows Mobile applications, iPhone applications.

Here is the scheme of generation and application of the dynamic passwords – Chip Authentication Program (CAP). At the entry of the algorithm the current number of the operation (ATC) and some other essential elements (i.e., random number, amount and currency of the transaction) are assigned, at the end of the algorithm the digital one-time password is generated, being the function of ARQC cryptogram (Authentication Request Application Cryptogram). The cryptogram is generated by means of «applied cryptogram calculation» algorithm defined in the EMV standard. In this algorithm the double-length (112 bites) Customer Master Key is used, being the only secret information transmitted to a mobile phone.

HTTPS-connection is established directly between the mobile phone and CIP Applic Ward loading Check-In-Phone Mobile Wallet to a mobile phone.

HTTPS-protocol will support:

- Authentication of Check-In-Phone central server communicated with Check-In-Phone Mobile Wallet at a mobile phone,
- Confidentiality and integrity of data exchange between the Application and the server.

Authentication of Check-In-Phone servers is executed with server SSL – certificate of the X.509 v.3 format obtained from VeriSign Certificate Center. Check-In-Phone AS is authenticated on the basis of the Common Name field of the AS servers certificate.

Confidentiality of the secret data for Check-In-Phone Mobile Wallet (Customer Master Key) during its loading and storage at a phone is provided by means of PBE cryptoalgorithm (Password – Based Encryption) described in PKCS#5v.2.2 standard. This cryptoalgorithm is realized in the frameworks of the standard package Bouncy Castle APIs for J2ME.
When keys are generated in PBE algorithm (3 DES algorithm is applied for data encrypting), the dynamic PIN-code and the Partners Application identification number (as a Salt value) are used.

Check-In-Phone offers a 2+factor authentication model to verify Check-In-Phone Users. In accordance with the model for successful authentication Check-In-Phone Users should:

- remember their dynamic PIN-codes for Check-In-Phone Applications;
- possess the operation from the mobile phone with a pre-defined subscribers number;
- use signed Check-In-Phone Mobile Wallet (a program-midlet) embedded in their mobile phones with a certain number.

A PIN-code is entered by Check-In-Phone User himself for each Application elaborated by Check-In-Phone Partner and is applied by the User every time the User is authenticated. The meaning of the PIN-code entered by the User is required to decrypt Customer Master Key that is kept encrypted in a mobile phone. That’s why having entered an incorrect PIN-code value owned by Check-In-Phone User in the process of decryption, the incorrect Customer Master Key value is obtained and that results in incorrect values of ARQC and one-time password. Three unsuccessful attempts to authenticate (incorrect value of the calculated cryptogram) lead to blocking Check-In-Phone Mobile Wallet of the particular User at the Authentication Server and the Mobile Wallet couldn’t be used more.

To check the phone number which has been used to download a certain Application into Check-In-Phone Mobile Wallet, Midlet specific SMS is used; this message is forwarded by the Check-In-Phone central server to the phone in accordance to the phone number stored in the database of the Check-In-Phone central server and is assigned for Mobile Wallet at this mobile phone. The Midlet specific SMS message contains a Challenge used within the CAP algorithm according to Model and Mode3 of the generation of one-time passwords (OTP).
In terms of security the most vulnerable stage of the Application’s life cycle is obviously a transmission of Check-In-Phone Wallet/Application and its personal data to a mobile phone. That’s why during Check-In-Phone Mobile Wallet loading to a phone the following mechanisms are applied:

- The download of Wallet and Partner’s Applications from CIP ApplicWard is realized with the use of HTTPS that provides confidentiality and integrity of data exchange between the server and the phone. Besides, when the Partner’s Application is downloaded confidential data of the Application (e.g., customer PIN-codes, Application download ticket) is forwarded to Check-In-Phone system encrypted under the public key of the Partner (Application’s Issuer). The RSA algorithm is used with the key module not less than 1024 bits.
- Customer Master Key is encrypted by means of the PBE algorithm (PKCS#5) based on 3DES algorithm. The key under which the Customer Master Key is encrypted, has a secret part – a PIN-code entered by the User and consisted of four digits. A fraudster has only three attempts to guess the PIN-code value. After the third unsuccessful attempt the Application is blocked in the Check-In-Phone system. This means that the probability to decrypt the Customer Master Key value is approximately equal to $3 \times 10^{-4}$.
- Check-In-Phone Mobile Wallet (a Jar-formatted file) is transmitted to a Check-In-Phone User mobile phone having been previously obfuscated. Obfuscation is assigned for reducing data size, renaming Check-In-Phone Mobile Wallet variables and even amending the instruction sequence in the source code. This implies that the swindler who intercepts a previously obfuscated Jar file can’t make sense of it. The file is then decompiled during its execution at a mobile phone owned by Check-In-Phone User.
- Check-In-Phone Mobile Wallet is signed by the CIP private key certified by VeriSign. If any Mobile Wallet is signed incorrectly, warning that information is received from an unreliable source is displayed on the phone’s screen, and every time the Mobile Wallet is used by the User, he is warned about its illegality. Check-In-Phone Mobile Wallet signing helps to authenticate DS additionally (besides HTTPS-protocol) and provide integrity of data transmitted to the User.

Check-In-Phone Mobile Wallet intercepted by swindlers couldn’t be used at other phones if Check-In-Phone Partner supports Check-In-Phone 2+-factor authentication.

The other attempt to compromise Check-In-Phone Wallet data is an interception of the OTP value generated by Check-In-Phone Mobile Wallet for which the encrypted value of Customer Master Key has been previously successfully intercepted. Examining all possible options of the dynamic PIN-code for the certain Check-In-Phone Application the values used for intercepted OTP value generation under the decrypted value of Customer Master Key may be defined. It may be proved that the probability, that the intercepted OTP value with the $K$ different values of PIN-code as the result of examination, will be equal to
\[
\sum_{k=1}^{K} \binom{n}{k} p^k (1-p)^{n-k} \\
1 - (1-p)^n
\]

where \( n \) is a number of different meanings of PIN-codes (when the PIN-code is a four-digit value, \( n = 10000 \)), \( p \) – the probability to obtain one value from \( n = 1000000 \) of equally possible OTP values. Substituting \( n \) and \( p \) values in the above equation, it’s easy to prove the probability that intercepted OTP value corresponds to a single meaning of PIN-code (\( K = 1 \)), is approximately equal to 0.9999.

If 2+-factor authentication is used, the intercepted Customer Master Key value of Check-In-Phone Mobile Wallet being the result of the abovementioned attack could be hardly realized.

Another risk should also be investigated: attacks aimed at an unauthorized access to the application confidential data stored in the phone memory. When Check-In-Phone Mobile Wallet is installed at a mobile phone, various files are generated for storing data related to Check-In-Phone Mobile Wallet and, particularly, Customer Master Key encrypted value. The File Management system in J2ME environment provides an opportunity for accessing files (generated as a result of the certain MIDlet installation, particularly, Check-In-Phone Mobile Wallet) from only this MIDlet.

According to the Practices Guide for MMA (prepared by MasterCard), Check-In-Phone Mobile Wallet clears up the memory of the mobile phone when it finishes operating. However Users should be warned by Partners that viruses can be loaded onto their mobile phones (like PCs). The viruses are capable to store crucial data stored in the main memory of the phone and transfer it to swindlers for examination. The viruses are capable of transferring the dynamic PIN-code value of the certain Application to swindlers.

At present nearly 300-400 viruses elaborated specially for mobile phones are known (e.g., database of viruses for personal computers is numbered several hundreds of thousands viruses). Yet no one is operating in the way described above. However, requirements to Partners and Users set by the Manager to comply with the recommended safety precautions measures must be met without fail. The noncompliance may result in corresponding restrictive measures imposed on breakers.

It’s important that every abovementioned attack (OTP intercepting with the already known encrypted Customer Master Key value, loading viruses-spies to the mobile phone owned by the User, scanning of PIN-code value and Customer Master Key value) allows a potential swindler to uncover only a single secret of the 2+-factor authentication. At the same time it’s very difficult to obtain access to all secrets.

That’s why the level of security of the Check-In-Phone scheme described above may be admitted as high. It may be stated with confidence that, for example, access to information about customers’ accounts as well as purchase operations for limited transaction amounts may be executed by means of Check-In-Phone Mobile Wallet. The risk of the financial operation is incurred to the client’s bank.
CIP provides confidentiality and integrity of information forwarded from the phone to the Bank’s server by means of standard tools. For this purpose when the Application of the Bank is initialized at the phone, a 3DES session key is generated and encrypted by the Bank public key. The encrypted key is transferred to CIP AG.

To provide secure data transfer between CIP AG and Bank’s server registered as Issuer a transportation key is used; the transportation key has been previously generated by the User and entered in the HSM of the Check-In-Phone system.

Besides, the results of any operation executed by any Bank may be signed by symmetric key of the Bank’s Application for the certain mobile phone. Thus the requirement of non-repudiation is met, as Check-In-Phone User can’t deny the transaction initiated by him (Non-repudiation).

Digital signature of the Application is generated according to the algorithm supported by MasterCard and Visa-CAP Mode2 with TDS. Up to 10 digital details of the operation could be signed according to this algorithm. The signature is executed by means of DES where the cryptogram is used as the key calculated by 3 DES and double key length Customer Master Key. Thus, crypto protection of the signature is equal to cryptographical security of 3 DES algorithm with the double key.

It’s worth to mention that no data about Application’s Users (Personal data) is stored in the Check-In-Phone system. Real details owned by Users (e.g., card number) are replaced by their substitutes (f.e., hash functions of the card number of other customer’s identifiers) in the Check-In-Phone system. Identifiers are transformed to the real details in banking system (f.e., to the card number) in CIP AP.

To summarize, following features can be used by the Bank’s Application to provide operations security:

2+-factor authentication of the User (Customer of the Issuer’s Application);
secure data exchange (central CIP servers’ authentication, confidentiality and data integrity) between a phone and CIP;
secure data exchange between the Bank’s Application on the phone and the Bank’s central system application;
a Customer is unable to deny the transaction he/she has executed (digital signature).

Russian Cryptography Standards Support

Check-In-Phone solution supports Russian cryptography standards called GOSTs. “Russian Digital Signature Standard” service provided to CIP Issuers and Users allows them remotely via mobile phone to carry out legal transactions confirmed by Electronic Digital Signature generated by Russian crypto algorithms. Digital Signature generation and verification is carried out according to the following cryptographic standards:
Russian Digital Signature Standard GOST P 34.11-94, Russian Digital Signature Standard GOST P 34.10-2001 and Russian Digital Signature Standard GOST P 28147-89

Russian Digital Signature Standard GOST P 34.10-2001 defines procedures of digital signature generation/verification based on elliptical curves. It replaced Russian Digital Signature Standard P 34.10-94. The digital signature is presented by a binary vector of 512 bits length. Digital signature cryptographical resistance is realized on the computational complexity of the computation of the discrete logarithm in the field of points of an elliptical curve. A hash-function is calculated in accordance to Russian Digital Signature Standard GOST P 34.11-94. The length of the meaning of the hash-function is 256 bytes.

Thereto the Client should enter the Issuer’s Application at the mobile phone and choose the corresponding menu item (GOST Support – DS) of the service menu in the Personal Office. Having chosen this item, the Client will get acquainted with the detailed description of the service. If the Client agrees to service conditions and terms, he’ll be offered (to Issuer’s discretion) either to use the existing PIN-code (PIN1) of Issuer’s Application (it should be entered), or use the additional PIN-code (PIN2) that should be invented by the Client and then entered twice before sending the request for service registration.

In this case PIN2 will be used only for DS (with Russian cryptography) generation. No matter how many PIN-codes (PIN1 or PIN2) the Client uses, two different keys encrypted at PIN are stored in the Application at a mobile phone. Two keys are as follows: the first one is used for one-time passwords generation and Client’s authentication, the second one – for DS (with Russian cryptography) generation when legal transactions are processed. The access to the private key for DS generation is closed by PIN2 in compliance with the Issuer’s security policies (entry attempts counter, number of symbols, etc.)

If registration and uploading have finished successfully, the system will inform the Client, and the Private Office menu item used for «GOST Support -DS» service registration will be deleted. From now all services where Russian cryptography is assigned by the Issuer will be available to the Client. The Client should enter PIN2 to get access to the service.

The sensitive data of the Issuer’s Application is stored encrypted at a mobile phone. The key of the Issuer’s Application used for one-time passwords generation and Client’s authentication is encrypted with the help of the Client’s PIN-code for this Application, however Client’s PIN-code and entry attempts counter are not stored at the phone. The signature key and verification key of the Issuer’s Application used for providing the Client with the additional «GOST Support- DS» cryptographic security are generated at a mobile phone. The signature key is encrypted with the Client’s PIN2-code for this Application and is stored encrypted in the Issuer’s Application. The main advantage of the proposed solution is that the key pair is generated by the User at a mobile device and the signature key never leaves the device. The security of the transactions processed is provided with encryption of sensitive data. The encryption will be used during:
data transfer from Issuer of the Application— at the session key generated by Issuer’s Application at a mobile phone and delivered to the Issuer as encrypted at the public key of the Issuer’s Application;

data transfer from the Application at a mobile phone to the Issuer’s server— at the public Issuer’s key session key.

Data integrity and its authenticity is provided during:

data transfer from Issuer of the Application – by means of control amount generated in response message CRC32 – data integrity or cryptographic signature (MAC) at the Issuer’s private key – data integrity and authenticity (option)
data transfer from Issuer’s Application at the phone – by means of control amount generated in response message CRC 32 and generation, if required, the data signature using MMA or Russian Digital Signature Standard.

The Issuer’s Application at the phone encodes the sensitive data by one of two keys:
the public key of the Issuer;
the session key. The session key is generated by Issuer’s Application and is delivered within the Application request to the receiving partner as encoded at the public key of Issuer.

The Issuer encodes transaction data at the session key that is generated by Issuer’s Application at the phone and is delivered to the Issuer encrypted at the Issuer’s public key. The Issuer’s private RSA key is stored in Issuer’s HSM. The Issuer’s public RSA key signed at the Wallet’s private key is stored at the phone.

Markup language (CIPML code) is used to design the User’s interface of the Issuer’s Application and description of services business-logic rendered to the Clients. CIPML-code received by Issuer’s Application is signed at the Issuer’s private key and is checked out at the Issuer’s public key before storing to a mobile phone. This key is loaded to the mobile phone when Issuer’s Application is personalized. CIPML-code, data and Issuer’s Application resources are delivered in separate blocks of the response message. This allows encoding (or signing) only sensitive data (the volume of which is less the CIPML-code and resources volume) thus helps saving time required for encoding operations.
Technological scheme of integration
CIP solution is integrated into the banking infrastructure for interaction in online mode.
The following components should be installed at the Issuer side:
- soft gateway: Check-In-Phone Access Point that is the interactor between CIP ApplicWard, personalization service, CIP Authentic Gate (authentication service), supporting service – telephone database and information systems of the Customer, that generates answers to Clients’ requests via Internet (Private office service) or through a mobile phone.
- CIP Authentic Gate – authentication service when transactions are processed
- CIP ApplicWard – service of mobile Application personalization
- Telephone database

![Technological scheme of integration](image)

The gateway supports several program adapters; each of them will allow supporting interface to the certain Client’s information system with specific set of intersystem transactions:
- Banking system,
- Processing system,
- CRM,
- Call-center
A set of Clients’ transactions (data transferred and received, the mode of transactions processing: simultaneous, isochronous, format presented in interfaces and at the phones) should be defined and determined.
The interface with the Customer’s banking system (personified Applications) may support a set of transactions, including but not limiting:
The company and the solution. Short review

- Payments to predefined banking details (using server of payments owned by the third-party developer):
  - paying for public utilities from the card or the current account;
  - billing payments (phone, internet, satellite broadcasting, etc.) from the card or the current account;
  - transferring money to the deposit from the card or the current account;
  - money withdrawal from deposit to the card or current account;
  - money transferring to investment funds from card or current account;
  - money withdrawal from investment funds to the current account, card;
- Payments to the optional banking details
  - transfer from the card or the current account to any Client of the other Bank.

- money transfer from the account to the account,
- money transfer from the account to Money Transfer Service System;
- money transfer between card accounts;
- money transfer between current accounts;
- money transfer between the card and the current account and vice versa;
- credit receiving (limit increasing) to one of the existing Client’s account (card, current account) without bank visiting (if this is provided by the remote service agreement);
- conversation operating;
- list of existing agreements (deposits, credits, investment funds share, card-related contracts), accounts, cards;
- existing agreements terms (as the details to the list of agreements);
- account balance;
- account balance, credit balance;
- credit repayment schedule;
- credit repayment schedule calculation to the definite date;
- investment funds current cost;
- estimation of investment funds yielding;
- Client’s payment ranking at the present moment taking into account currencies, income and expenses;
- Client’s ranking taking into account portfolio and stocks;
- Client’s personal payment register;
- contact information of the manager assisted the Client

The interface with the processing system (personified Applications) may support the following set of transactions:

- means at Client’s card available to authorization;
- money blocked (“hold”) and not processed from the card;
- list of transactions processed;
- reference on the current or previous settlement period;
- card blocking;
- **card unblocking that was prior blocked with the status “blocking the card remotely by the Client”**;
- card ordering/refusal for card reissuing;
- fixing/altering limit on card;
- additional services switching on (sms-informing and etc.);
- card/account closing;
- payments to the predefined bank details;
- Application for the card issuing.

The interface with CRM (personified Applications) may support the following set of transactions, required confirmation in the exchange protocol, including but not limiting:
- bank’s messages (letters) addressed to the Client;
- Applications for fixing/altering of credit limit/credit (consumer credit, autocredit, mortgage credit, etc);
- Applications for brokerage services rendering, marginal operations;
- agreements and operational documents signing (print the credit agreement, sign it and visit the nearest Bank’s office);
- scoring /underrating remotely, obtaining the confirmation, then, when successful, printing the Agreement and visit the Bank;
- communication with the manager-inquires, answers, requests for goods/services;
- correction of the personal payment register.

The interface with Call-centre (nonpersonified services) may support the following set of transactions, required confirmation in the exchange protocol, including but not limiting:
- reference on tariffs, services, standard agreements, calculators, types of credits, products description,
- bank’s offices addresses, ATM with location map and operating hours,
- partners-corporate Clients, their offices, goods and services,
- news:
  - Date of news,
  - Subject of news,
  - Text of news in html format,
  - Forwarding to the optional link for the detailed description,
  - Web-site events (f.e., Bank’s site),
  - The importance of news.
- Advertising services,
- Administrating information.
8. Integration with the Client’s Call-centre. Main issues

CIP provides a comfortable and reliable algorithm relating to the Client’s authentication at the moment a client applies to the contact-centre (Call-centre) for personified services obtaining.

CIP is rather than technology allowing reliable Client’s authentication, it helps identifying the Client automatically as well as the service requested by him at the moment he applies to the Call-centre from a mobile phone.

There are two ways of the mobile Client’s authentication when applying Call-centre for obtaining the service offered by the Partner:

- from a stationary phone
- from a mobile phone

- Client’s authentication is realized by CIP AuthenticGate service. The information required for the authentication is transferred from Call-centre in one of the following ways: by Call-centre operator by means of WEB-Application (WEB-Client) that interacts with Check-In-Phone AuthenticGate service via CIP Access Point at the Client’s side;
- by Call-centre Application that will accept the call from the Client’s phone and deliver the request to the CIP AuthenticGate service automatically via CIP Access Point at the Client’s side (preferably).

At the stationary phone, authentication may be realized:
- during voice data transferring,
- during tone data dialing.

Call-center operator involvement into the request generation to the CIP AuthenticGate service is different though the above algorithms are the same.
**Client’s authentication during voice data transferring**

The service is rendered by Call-centre to the Client who applies from the stationary phone.

a) The Client uses a mobile phone as cryptocalculator for OTP (one time password) generation. With that end in view he chooses the menu item in CIP Application at a mobile phone relating to OTP generation, enter the mobile PIN –code of this Application and OTP is generated.

b) The Client phones the Call-centre from the stationary phone and informs the operator of:
   - Application name (option),
   - Service code (option, if the service is chosen before authorization),
   - Client’s identifier (mobile’s phone number),
   - One-time password (OTP).

The information obtained from the Client by means of WEB-Application is included manually by the operator to the request and is forwarded to CIP AG by means of the secured channel.

c) CIP AG service checks OTP and generates the response message.

d) Call-centre Application checks the authentication result from the response message and the response message signature. When the result is a success the Client obtains access to the Bank’s service.

e) Call-centre keeps stored all response messages signed by CIP AG service in case of dispute situations. The requirements for data storage time are defined additionally.
**Client’s authentication without Call-centre operator during tone data dialing**

The authentication is carried out like the previous script, excluding the options:
- Application name (option)
- Service code (option, if the service is chosen before authorization)
- Client’s identifier (mobile’s phone number)
- One-time password (OTP)

are dialed up in tone mode, and the request is generated and forwarded to the CIP AG service automatically without call-centre operator.

**Client’s authentication when the Client uses a mobile phone to access the service**

The Client uses Call-centre services from a mobile phone with the predefined mobile Check-In-Phone Wallet and Bank’s Application.

- The Client chooses CIP Application menu item in the mobile CIP Wallet relating to the service obtaining through Call-centre. The Application at a mobile phone after entering the mobile PIN-code by the Client generates OTP.
- Then the Bank’s Application at a mobile phone connects with the Call-centre through the fixed number and forwards the message 1 (see picture) OTP and additional information within a DTMF-sequence:
  - Application name (option),
  - Service code (option, if the service is chosen before authorization),
  - Client’s identifier.
In some cases the Client’s identifier may be defined by the mobile number, that the Call-centre defines with the help of the automatic number identification (ANI).

c) Call-centre Application transforms the data received from the Client into the request delivered to the CIP AG service (2).

d) CIP AG service checks OTP and generates the response message (3). The response message is signed by CIP AG server.

e) Application at the Call-centre intelligent platform, having received the response message, checks the results of the Client’s authentication and response message signature. If the result is a success the Client gets access to the Partner’s service.

f) Call-centre stores the response messages signed by CIP AG server in case of dispute situations.

g) Call-centre Application depending on the code of the service requested by the Client (if required) may inquire the necessary information in Informational System (IS) of the Partner (4). For example, if there is the service code “Balance inquiry”, the request to the Client’s account is made.

h) The results of this request (5) are then forwarded to the Partner’s Client during its telephone dialog (6) with the Call-centre operator.
9. One-time passwords for Internet-banking checking

OTP generator is a unique means for Users’ verification for the Bank. One-time password may be delivered to CIP AuthenticGate for checking automatically (from a mobile phone to AS Check-In-Phone through the secure channel) as well as “by eyes and hands” (OTP and identifier are carried out manually or by voice from phone’s screen to other informational system for the further checking through AS Check-In-Phone).

For OTP generation the User will enter CIP Wallet’s menu, then Application’s menu and choose the icon “One-time password” of this Application.

After that the window appears at the phone’s screen it prompts the User to enter mobile PIN-code. After PIN-code is entered the digital value of the calculated OTP appears at the phone’s screen, if the Application provides, for example, when the data is transferred from a mobile phone to the informational system manually. In the other cases the Application will communicate with OTP on it's own, not showing the value to the User that is transparent for him.

OTP value is defined pursuant to Chip Authentication Program standard well known to MasterCard Worldwide and Visa International.

The User can apply generated OTP passwords to access various services channels. For example, a User can calculate a one-time password to access Internet-banking.

*The most comfortable solution is CIP usage at a mobile phone as means of transactions verification initiated through the other channels, for instance, through Internet-banking. At this, the one-time password is generated and used in the transparent for the Client way.*
The script of the following algorithm is presented below:

1) The Client enters his login on the WEB-page of the Internet-banking and some ID (for instance, the number of the mobile phone) using a browser of the personal computer and send the request for accessing to the system.

2) CIP Access Point gets the client’s request and sends it to the phone of this User to the mobile Application to obtain the verification (the random number (Challenge) may be used, that is delivered to the entry of the mobile Application at the Client’s phone)

3) The Client is waiting for the verification request, and having received it, enters the mobile PIN-code, based on which the response, including OTP (one-time password, being the signature in fact, including the processed cryptographically the Challenge meaning) is generated and delivered, being the result of the cryptographic processing of the entry data by the mobile Application.

4) CIP Access Point forwards the received OTP to the verification center: CIP AuthenticGate.

5) CIP AuthenticGate checks OTP and forward the verification result to CIP Access Point.
6) CIP Access Point forwards the request to the banking system for generating of the response to the Client or executing his instructions.

7) The banking system processes the request and generates the answer for the Client, forwarded to CIP Access Point.

8) CIP Access Point sends the response to the Client’s browser.

The above algorithm presents a shared secret, generated by the Application at the phone and provides the Client with the comfort because it excludes OTP manual entry mistakes.
10. **Check-In-Phone: transactions with authentication made with banking cards**

For large amount transactions made with banking cards and processed at ATMs and POS terminals, anti-skimming activity may be additionally strengthened by the Client’s confirmation that it’s his initiative to process the transaction.

Check-In-Phone solution makes a Client capable to confirm by phone (by entering mobile PIN-code and generating the transaction cryptogram) his initiative to process the transaction. To that end, an algorithm similar to the EMV banking card algorithm is performed. An additional request is embedded into the authorization process for obtaining the Client’s confirmation with the help of CIP Application at his mobile phone.

The Client knows that the operation with confirmation is processed, he gives the card to the cashier (inserts it into the ATM’s slot and etc.) and initiates the transaction.

The Client uploads the Check-In-Phone mobile Application and, after having entered mobile PIN-code, he obtains access to CIP mail, uploads the request for confirmation of the transaction, and enters the PIN-code once again. The generated cryptogram is used as a confirmation for the transaction performed.

Authorization process of the Issuer’s processing system completes the authorization and sends the authorization response to the acquirer host. The Client will get the service (goods, money).
Client authentication is widely required in card technologies. Different kinds of authentication are used depending on delivery channels of remote services. For instance, PIN-code is widely used to authenticate a Client during withdrawal operations at ATM; code words (alpha-numeral sequences) are used for card blocking/unblocking or service obtaining through telephone banking; static passwords are frequently used in e-commerce. Reliable authentication is extremely important when a bank wants to train its Clients not to visit branches and render them services remotely.

At present two trends are observed in Client’s authentication – 1) the desire to unify the authentication procedure for all service delivery channels and 2) distrust to static passwords (the most widely spread way of the Client’s authentication) as less reliable authentication method. The first trend is based on the Client’s desire to use a single procedure of his identification/authentication that makes his life easier - you shouldn’t remember numerous passwords/codes/identifiers to get access to various banking products.

The second trend is also reasonable. A static password is given one time for the significant period of time and may be stolen and used by swindlers for obtaining services on behalf of the Client. The password entered at the computer’s keyboard may be stolen by means of the special “programs-spies” downloaded to the Client’s computer. These program-spies can trace data typed by the Client at the keyboard (keyboard logger). Last years a lot of headache is given by phishing when swindlers send the requests to the Clients via e-mail on behalf of their banks asking them their personal data renewal.

Some special schemes assign the most advanced technologies of passwords stealing (vishing, farming and etc.). For instance, when using a static password for Internet-banking it may happen that the static password is intercepted by swindlers who are placing themselves between the Client’s computer and Internet-banking server (‘‘Man in the Middle attack’’). The Client during this attack can see the fraudulent entry page and his password is intercepted.
As a result a swindler using the intercepted Client’s password can transfer client’s money from his account.

To protect from the static passwords stealing different schemes of dynamic passwords (or one-time passwords-OTP) are offered. One of the wide spread OTP generation algorithm is Chip Authentication Program (CAP) elaborated by MasterCard and accepted by VISA under the brand name Dynamic Passcode Authentication (DPA).

To realize the CAP/DPA method a Client should obtain the chip card with EMV application as well as a special personal card reader capable to initiate OTP password generation and display its value consisting of 6-16 digits at the reader’s screen.

CAP/DPA method is a two-factor method. This means that to obtain a correct OTP the chip card presence and correct PIN entry are required.

There are three variants of CAP/DPA methods:
1) Identify-OTP is generated without entering any additional data;
2) Response—the Client is said some random number that he should enter to the reader (challenge), and then the Client gets the OTP value.
3) Sign—the extension of the previous method, where a Client should enter some crucial transaction data, for instance, amount and the currency of the transaction, account number and etc. Different variants of this method may be applied to different banking solutions. This method may be extremely popular with a bank and several banking services may use this method simultaneously:
   o Internet-banking (entrance, order confirmation);
   o Call-centre (the calling person identification);
   o Merchant acquiring made with cards in Internet (3-D secure method developing);
   o Big amount payments confirmation;
   o Brokerage service (orders assurance);
   o Application accepting to connect chargeable services.

At present more than 22 mln readers are sold (delivered) in Europe. 20 mln of them are used for Internet-banking, nearly 2 mln are used for additional options. From 70 banks using the above method there are 6 biggest English banks (RBS, Barclays, Rabo-bank, ABN-AMRO, etc.) and the Swedish Nordea.

Check-In-Phone solution based on CAP is able to verify OTPs generated according to CAP. This ability adds CIP the additional functional opportunity to replace a solution consisting of EMV card and reader for CAP generation with the following verification by the CIP system.
12. **Check-In-Phone: money transfer and cash withdrawal in ATM or branch without the card**

Check-In-Phone allows its Customer to realize the system of electronic money transfer initiated from the phone of the payer. The receiver then may receive the money without banking card or account with the help of the ATM, SST (self-service terminal) and Bank’s branches.

The sender-the Client of the CIP Customer-may transfer the amount within the limit defined by the Customer, in ATM or SST owned by the Customer and the Banks-partners.

The sender is first required to enter the telephone number of the receiving party, amount and PIN-code. The generated by the CIP application CAP is used by the central system for authenticate a sender and form new payment transfer in the system. As the answer to the sender’s request, the CIP central system will forward to the mail agent of the Check-In-Phone Application at the receiver’s mobile phone the number, amount and payment secret code (to Customer’s discretion), and at the mail agent of the mobile Application at the sender’s mobile phone the notification of successful transfer generation.

ATM screens should be equipped by the screen “Cash withdrawal within the Check-In-Phone service”, ATM configuration is realized allowing their operation in non-card mode, as well as the minimum changes in exchange protocols and authorization processes of the Customer’s processing system.

The receiver will press the button of the ATM that will automatically activate it for transactions within Check-In-Phone service.

After that the receiver is able to withdraw the cash with the help of the number, access code and the amount notification. The partial cash withdrawal isn’t recommended. The amount not demanded by the receiver can be returned to the sender’s account if the term defined by the sender is elapsed.
13. Check-In-Phone services configuration

The solution procured provides an opportunity to configure Client’s Applications. Using CIP AG and CIP AW a Bank has an opportunity to

- Create and support an unlimited number of mobile Applications which are characterized by the following features:
  - Individual set of Client services (menu items of the mobile Application),
  - Individual data for Client identification,
  - Individual secret data,
  - Bank’s server URL,
  - Preferred language of the interface with the Check-In-Phone User (Russian by default),
  - CAP profile.

- Define groups of Clients with access to downloading, activating and usage of mobile Applications of the certain category,

- Block mobile Applications,

- Change access to the operations within the Application life cycle: add, delete, alter services (without the Application uploading by means of the CIPML service menu renewing with notification to the Client),

- Provide access to the full set of the services via Internet using Applications as crypto calculators which calculate one-time passwords according to CAP for mobile telephones (MMA). These OTPs are then entered as passwords to access services via Internet,

- Provide Clients with an opportunity to set up menu items of the personal mobile Application from their phones and service menu of the Personal Office in Internet. Any time a Client may undertake the reconfiguration of the User’s menu for its compliance with personal needs.
14. Support and compatibility

Here are the main functional opportunities, architecture and interfaces used by Check-In-Phone help desk (CIP-HD). CIP-HD is intended for information providing, Check-In-Phones clients’ applications and claims processing.

CIP-HD provides the following key functions realization:
• Telephone database maintenance;
• Existing telephone database support, its renewal and errors correction;
• Mobile phones testing to ensure system compatibility;
• Clients registration in compliance with the system requirements;
• Managing of access and clients’ system accounts;
• Transactions logging;
• Receiving and processing requests for technical support from the registered members of the system;
• Based on the received requests preparing of the information required by the clients of the system;
• Requests (electronic documents) delivery to the technical support centre for the further processing and preparing answers.

CIP-HD has obtained three-level architecture:
• Call-centre/WEB;
• first-level technical support;
• second-level technical support.

Call-centre/WEB
Key functions:
• Events logging (client calls or WEB requests):
  - time of the call and telephone number;
  - phone model definition (using phone database as an assistant for model definition);
  - cellular operator definition (using phone database as an assistant for model definition);
  - short description of the problem;
  - call time and contact information specification, when and where an answer to the client should be sent via e-mail.
• Simple answers to the general questions (FAQ – I).
• Informing the clients/sending the answers to clients’ requests prepared by first-level and second-level technical support.

First-level technical support
Main functions:
• Analysis, definition and identification of the problems fixed by the CIP-HD;
• Problem status definition according information from the production
environment (telephone model, what applications/profiles are uploaded to the client, list of possible problems for this model);
- Preparation and forwarding by e-mail an answer to the client or call-centre (reference to the “electronic” answer);
- Assistance in GPRS activation (obtaining GPRS settings);
- Assistance in midlet uploading according to the telephone model and answer to the questions that haven’t got simple answers (FAQ-II);
- Assistance in questions related to the Wallet’s and Issuer’s applications.
- Main task - preparation of written or verbal answers to the call-centre questions.
- Elaboration of the electronic standard answers (FAQ-I and FAQ-II).

Second-level technical support

Main functions:
- analysis of the problems relating to CIP operation at "bad" telephones and during worst-case situations;
- assistance in answers preparing for questions that haven’t been answered by first-level technical support specialists.

The main task - provide the opportunity for elaboration/preparation new electronic standard messages according to FAQ-I and FAQ-II. Providing the opportunity to obtain client’s status information from the production environment.

Database contents and structure.

Help Desk database includes reference tables obtained from the outer source and tables prepared during system elaboration and system maintenance.

Reference tables:
- Telephone manufacturers reference table;
- Telephones reference table;
- Cellular operators reference table including operators codes;
- GPRS settings reference table for various manufacturers and telephone models.

Tables prepared during system elaboration and system maintenance:
- Electronic standard answers reference table (FAQ-I);
- Electronic standard answers reference table (FAQ-2);
- Detected problems table;
- Table of Call-centre operators requests to the central Check-In-Phone relating the questions haven’t been answered by operators and central Check-In-Phone answers.

The short description of the information containing in tables is below

1. Reference tables
   1.1 Telephone manufacturers reference table The reference includes the names of the main telephone manufacturers, the data is present in mobile phones databases.
   1.2 Telephones reference table consists of nearly 1300 models information, it also includes data received from manufacturers or some other sources required for possible
telephone usage in Check-InPhone system:
- Telephone model;
- Platforms supported (Java, Widows Mobile, iPhone);
- Java support (MIDP and CLDC);
- GPRS support.

Supported telephones database is presented in Appendices 2 and 3.

1.3 Cellular operators reference table including operators codes. The reference table contains lookup table “telephone number-cellular operator”

1.4 GPRS settings reference table for various manufacturers and telephone models. The reference table contains the information required for GPRS setting up at the clients’ mobile phones.

2. Tables prepared during system elaboration and system maintenance.

2.1 Electronic standard answers reference table (FAQ-I).
Contains the list of electronic standard answers to the questions that clients may have during application uploading and Check-In-Phone and Issuer’s applications operating:
- How to detect the phone’s model
- How to define Internet-GPRS settings
- Where is SMS received
- How to follow the link for downloading after receiving SMS
- Where is a WAP-push message
- Where is the loaded application
- How to find the information about the application
- How to set up access permissions allowing application to enter Internet
- How to find the information about PKI certificates
- Standard answers to the questions on the Check-In-Phone application
- Standard answers to the questions on the Issuer’s application

2.2 Electronic standard answers reference table (FAQ-II). Includes the list of electronic standard answers to the questions that haven’t got simple answers

2.3 Detected problems table. The table contains problem’s description, revealed during the system operation enlisted together with the status of the problem.

2.4 Table of the telephones testing results. The table contains the results of the mobile telephones testing for the purpose system compatibility, carried out as the result of the special investigation and testing in production environment.

2.5 Regitrated clients table. Contains the list of registered clients with the questions asked by the clients, status of the questions asked, contact information, data and ID electronic standard answers forwarded to the client.

2.6 Table of operations. Contains log of operations, processed by CIP-HD

**Telephones produced by main manufacturers and supported by CIP system**

Statistics of telephones produced by the main manufacturers and maintained in CIP database is below, Table 1.
Table 1 Telephones supported by CIP system

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Models (total)</th>
<th>Supported</th>
<th>%</th>
<th>Not supported</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>SonyEricsson</td>
<td>141</td>
<td>118</td>
<td>83,7</td>
<td>23</td>
<td>16,3</td>
</tr>
<tr>
<td>Nokia</td>
<td>225</td>
<td>119</td>
<td>52,9</td>
<td>106</td>
<td>47,1</td>
</tr>
<tr>
<td>LG</td>
<td>124</td>
<td>76</td>
<td>61,3</td>
<td>48</td>
<td>38,7</td>
</tr>
<tr>
<td>Motorola</td>
<td>161</td>
<td>84</td>
<td>52,2</td>
<td>77</td>
<td>47,8</td>
</tr>
<tr>
<td>Samsung</td>
<td>242</td>
<td>142</td>
<td>58,7</td>
<td>100</td>
<td>41,3</td>
</tr>
<tr>
<td>Total</td>
<td>893</td>
<td>539</td>
<td>60,4</td>
<td>354</td>
<td>39,6</td>
</tr>
</tbody>
</table>

Notes: How the decision is made whether java application Check-In-Phone is supported by the client’s telephone:
1 Supported: 1) Java support: MIDP2.0 and higher, CLDC1.0 and higher. 2) GPRS support.
2 Not supported: one of the conditions enlisted in issue 1 is not carried out.

List of telephone models produced by main manufacturers and supported by Check-In-Phone system

Table 2 Manufacturer: LG. Models:

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Models</th>
<th>Models supported</th>
<th>%</th>
<th>Models not supported</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>770</td>
<td>B2100</td>
<td>C1100</td>
<td></td>
<td>C1200</td>
<td></td>
</tr>
<tr>
<td>KE500</td>
<td>F3000</td>
<td>KE9850</td>
<td></td>
<td>HB620T</td>
<td></td>
</tr>
<tr>
<td>KE770</td>
<td>F9100</td>
<td>KE9970</td>
<td></td>
<td>KE990/990D</td>
<td></td>
</tr>
<tr>
<td>KF300/KF300D</td>
<td>KS310/311</td>
<td>KS390</td>
<td></td>
<td>KS510</td>
<td></td>
</tr>
<tr>
<td>KF750</td>
<td>KS360</td>
<td>KT520</td>
<td></td>
<td>KT525</td>
<td></td>
</tr>
<tr>
<td>KG280</td>
<td>KS450</td>
<td>KS800</td>
<td></td>
<td>KS990</td>
<td></td>
</tr>
<tr>
<td>KM500</td>
<td>KG290</td>
<td>KG320</td>
<td></td>
<td>KG920</td>
<td></td>
</tr>
<tr>
<td>KP233</td>
<td>KG210</td>
<td>KG800</td>
<td></td>
<td>KG300D</td>
<td></td>
</tr>
<tr>
<td>KS20</td>
<td>KG290</td>
<td>KG320</td>
<td></td>
<td>KG920</td>
<td></td>
</tr>
<tr>
<td>KU380/KU385</td>
<td>KG210</td>
<td>KG800</td>
<td></td>
<td>KG920</td>
<td></td>
</tr>
<tr>
<td>M4300</td>
<td>KG290</td>
<td>KG320</td>
<td></td>
<td>KG920</td>
<td></td>
</tr>
<tr>
<td>S5200</td>
<td>KG290</td>
<td>KG320</td>
<td></td>
<td>KG920</td>
<td></td>
</tr>
<tr>
<td>U8200</td>
<td>KG290</td>
<td>KG320</td>
<td></td>
<td>KG920</td>
<td></td>
</tr>
</tbody>
</table>

Table 3 Manufacturer: Motorola. Models:

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Models</th>
<th>Models supported</th>
<th>%</th>
<th>Models not supported</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1000</td>
<td>A1010</td>
<td>A1200</td>
<td></td>
<td>A1600</td>
<td></td>
</tr>
<tr>
<td>A668</td>
<td>A760</td>
<td>A768</td>
<td></td>
<td>A768</td>
<td></td>
</tr>
<tr>
<td>A845</td>
<td>AURA</td>
<td>C385</td>
<td></td>
<td>C168</td>
<td></td>
</tr>
<tr>
<td>C380</td>
<td>C385</td>
<td>C390</td>
<td></td>
<td>C250</td>
<td></td>
</tr>
<tr>
<td>C980</td>
<td>E1000</td>
<td>E1060</td>
<td></td>
<td>E1120</td>
<td></td>
</tr>
<tr>
<td>E398</td>
<td>E550</td>
<td>E680</td>
<td></td>
<td>E680</td>
<td></td>
</tr>
<tr>
<td>E985</td>
<td>i860</td>
<td>i2</td>
<td></td>
<td>1,7</td>
<td></td>
</tr>
<tr>
<td>MOTOKRZ R K1m</td>
<td>MOTOKRZ</td>
<td>MOTORAZR</td>
<td>Moto</td>
<td>MOTORIZR Z3</td>
<td>MOTORIZR Z6</td>
</tr>
<tr>
<td>E608</td>
<td>MOTOSLVR</td>
<td>L1,9</td>
<td>Moto</td>
<td>MPx300</td>
<td>MPx200</td>
</tr>
<tr>
<td>RAZR V3</td>
<td>RAZR V3i DG</td>
<td>RAZR V9</td>
<td>Moto</td>
<td>V1050</td>
<td>V176</td>
</tr>
<tr>
<td>V188</td>
<td>V220</td>
<td>V235</td>
<td></td>
<td>V270</td>
<td></td>
</tr>
<tr>
<td>V360</td>
<td>V350</td>
<td>V355</td>
<td></td>
<td>V505</td>
<td></td>
</tr>
<tr>
<td>V550</td>
<td>V555</td>
<td>V975</td>
<td></td>
<td>V557</td>
<td></td>
</tr>
<tr>
<td>V635</td>
<td>V80</td>
<td>V975</td>
<td></td>
<td>V980</td>
<td></td>
</tr>
<tr>
<td>3100 Classic</td>
<td>3220</td>
<td>3230</td>
<td></td>
<td>3250</td>
<td></td>
</tr>
<tr>
<td>3110 Classic</td>
<td>3220</td>
<td>3230</td>
<td></td>
<td>3250</td>
<td></td>
</tr>
</tbody>
</table>

Table 4. Manufacturer: Nokia. Models:

<table>
<thead>
<tr>
<th>Model</th>
<th>Model</th>
<th>Model</th>
<th>Model</th>
<th>Model</th>
<th>Model</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>2600</td>
<td>2610</td>
<td>2626</td>
<td>2630</td>
<td>2760</td>
<td>3109</td>
<td></td>
</tr>
<tr>
<td>3110</td>
<td>3220</td>
<td>3230</td>
<td>3250</td>
<td>3500</td>
<td>3610</td>
<td></td>
</tr>
<tr>
<td>3610 fold</td>
<td>5000</td>
<td>5070</td>
<td>5130 XpressMusic</td>
<td>5140</td>
<td>5200</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>------</td>
<td>------------------</td>
<td>------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>5300</td>
<td>5310 XpressMusic</td>
<td>5500</td>
<td>5700 XpressMusic</td>
<td>5800 XpressMusic</td>
<td>6020</td>
<td></td>
</tr>
<tr>
<td>6021</td>
<td>6030</td>
<td>6060</td>
<td>6061</td>
<td>6070</td>
<td>6085</td>
<td></td>
</tr>
<tr>
<td>6086</td>
<td>6101</td>
<td>6102</td>
<td>6103</td>
<td>6108</td>
<td>6110 Navigator</td>
<td></td>
</tr>
<tr>
<td>6111</td>
<td>6120 Classic</td>
<td>6124</td>
<td>6125</td>
<td>6131</td>
<td>6136</td>
<td></td>
</tr>
<tr>
<td>6151</td>
<td>6170</td>
<td>6212 Classic</td>
<td>6220 classic</td>
<td>6230</td>
<td>6230i</td>
<td></td>
</tr>
<tr>
<td>6233</td>
<td>6236i</td>
<td>6260</td>
<td>6270</td>
<td>6280</td>
<td>6288</td>
<td></td>
</tr>
<tr>
<td>6290</td>
<td>6300</td>
<td>6301</td>
<td>6500 Classic</td>
<td>6650</td>
<td>6670 Slide</td>
<td></td>
</tr>
<tr>
<td>6600</td>
<td>6620</td>
<td>6630</td>
<td>6660</td>
<td>6670</td>
<td>6680</td>
<td></td>
</tr>
<tr>
<td>6681</td>
<td>6682</td>
<td>6822</td>
<td>7070 Prism</td>
<td>7200</td>
<td>7260</td>
<td></td>
</tr>
<tr>
<td>7270</td>
<td>7360</td>
<td>7370</td>
<td>7390</td>
<td>7500 Prism</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7610</td>
<td>7700</td>
<td>7710</td>
<td>7900 Prism</td>
<td>8600 Luna</td>
<td>8800</td>
<td></td>
</tr>
<tr>
<td>8801</td>
<td>9300 Communicator</td>
<td>9300i Communicator</td>
<td>9500 Communicator</td>
<td>E50</td>
<td>E51</td>
<td></td>
</tr>
<tr>
<td>E61</td>
<td>E61i</td>
<td>E62</td>
<td>E63</td>
<td>E65</td>
<td>E66</td>
<td></td>
</tr>
<tr>
<td>E70</td>
<td>E71</td>
<td>E90 Communicator</td>
<td>N70</td>
<td>N71</td>
<td>N72</td>
<td></td>
</tr>
<tr>
<td>N73</td>
<td>N75</td>
<td>N76</td>
<td>N77</td>
<td>N78</td>
<td>N80</td>
<td></td>
</tr>
<tr>
<td>N81</td>
<td>N82</td>
<td>N85</td>
<td>N90</td>
<td>N91</td>
<td>N92</td>
<td></td>
</tr>
<tr>
<td>N93</td>
<td>N93i</td>
<td>N95</td>
<td>N96</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 5. Manufacture: Samsung. Models:

<table>
<thead>
<tr>
<th>Model</th>
<th>Model</th>
<th>Model</th>
<th>Model</th>
<th>Model</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>SGH-A737</td>
<td>SGH-C130</td>
<td>SGH-C140</td>
<td>SGH-C170</td>
<td>SGH-C200</td>
<td>SGH-C207</td>
</tr>
<tr>
<td>SGH-C210</td>
<td>SGH-C225</td>
<td>SGH-C230</td>
<td>SGH-C240</td>
<td>SGH-C250</td>
<td>SGH-C260</td>
</tr>
<tr>
<td>SGH-C300</td>
<td>SGH-C520</td>
<td>SGH-D307</td>
<td>SGH-D357</td>
<td>SGH-D410</td>
<td>SGH-D415</td>
</tr>
<tr>
<td>SGH-D488</td>
<td>SGH-D500</td>
<td>SGH-D500E</td>
<td>SGH-D510</td>
<td>SGH-D520</td>
<td>SGH-D550</td>
</tr>
<tr>
<td>SGH-D600</td>
<td>SGH-D700</td>
<td>SGH-D710</td>
<td>SGH-D720</td>
<td>SGH-D730</td>
<td>SGH-D800</td>
</tr>
<tr>
<td>SGH-D820</td>
<td>SGH-D830</td>
<td>SGH-D840</td>
<td>SGH-D880</td>
<td>SGH-D900</td>
<td>SGH-D900i</td>
</tr>
<tr>
<td>SGH-E105</td>
<td>SGH-E105</td>
<td>SGH-E200</td>
<td>SGH-E250</td>
<td>SGH-E300</td>
<td>SGH-E310</td>
</tr>
<tr>
<td>SGH-E317</td>
<td>SGH-E335</td>
<td>SGH-E340</td>
<td>SGH-E360</td>
<td>SGH-E370</td>
<td>SGH-E380</td>
</tr>
<tr>
<td>SGH-E390</td>
<td>SGH-E410</td>
<td>SGH-E420</td>
<td>SGH-E480</td>
<td>SGH-E490</td>
<td>SGH-E500</td>
</tr>
<tr>
<td>SGH-E530</td>
<td>SGH-E570</td>
<td>SGH-E590</td>
<td>SGH-E600</td>
<td>SGH-E610</td>
<td>SGH-E620</td>
</tr>
<tr>
<td>SGH-E640</td>
<td>SGH-E710</td>
<td>SGH-E715</td>
<td>SGH-E720</td>
<td>SGH-E730</td>
<td>SGH-E740</td>
</tr>
<tr>
<td>SGH-E750</td>
<td>SGH-E760</td>
<td>SGH-E770</td>
<td>SGH-E780</td>
<td>SGH-E790</td>
<td>SGH-E810</td>
</tr>
<tr>
<td>SGH-E830</td>
<td>SGH-E840</td>
<td>SGH-E870</td>
<td>SGH-E900</td>
<td>SGH-E910</td>
<td>SGH-E950</td>
</tr>
<tr>
<td>SGH-F300</td>
<td>SGH-F490</td>
<td>SGH-F500</td>
<td>SGH-G600</td>
<td>SGH-G800</td>
<td>SGH-G810</td>
</tr>
<tr>
<td>SGH-I250</td>
<td>SGH-I300</td>
<td>SGH-I500</td>
<td>SGH-I505</td>
<td>SGH-I530</td>
<td>SGH-I550</td>
</tr>
<tr>
<td>SGH-I700</td>
<td>SGH-I750</td>
<td>SGH-I600E</td>
<td>SGH-I-M300</td>
<td>SGH-I-P207</td>
<td>SGH-I-P310</td>
</tr>
<tr>
<td>SGH-P400</td>
<td>SGH-P410</td>
<td>SGH-P510</td>
<td>SGH-P705</td>
<td>SGH-P710</td>
<td>SGH-P738</td>
</tr>
<tr>
<td>SGH-P738</td>
<td>SGH-P850</td>
<td>SGH-P860</td>
<td>SGH-I-U100</td>
<td>SGH-I-U300</td>
<td>SGH-I-U600</td>
</tr>
<tr>
<td>SGH-U700</td>
<td>SGH-I-U900</td>
<td>SGH-X160</td>
<td>SGH-X200</td>
<td>SGH-X300</td>
<td>SGH-X450</td>
</tr>
<tr>
<td>SGH-X548</td>
<td>SGH-X475</td>
<td>SGH-X480</td>
<td>SGH-X510</td>
<td>SGH-X520</td>
<td>SGH-X530</td>
</tr>
<tr>
<td>SGH-X540</td>
<td>SGH-X620</td>
<td>SGH-X630</td>
<td>SGH-X640</td>
<td>SGH-X650</td>
<td>SGH-X660</td>
</tr>
<tr>
<td>SGH-X670</td>
<td>SGH-X680</td>
<td>SGH-X700</td>
<td>SGH-X800</td>
<td>SGH-X810</td>
<td>SGH-X820</td>
</tr>
<tr>
<td>SGH-Z100</td>
<td>SGH-Z105</td>
<td>SGH-Z107</td>
<td>SGH-Z130</td>
<td>SGH-Z300</td>
<td>SGH-Z500</td>
</tr>
<tr>
<td>SGH-Z540</td>
<td>SPH-A900</td>
<td>SPH-A920</td>
<td>SPH-A900</td>
<td>SPH-A920</td>
<td>SPH-A920</td>
</tr>
<tr>
<td>SGH-A737</td>
<td>SGH-C130</td>
<td>SGH-C140</td>
<td>SGH-C170</td>
<td>SGH-C200</td>
<td>SGH-C207</td>
</tr>
<tr>
<td>SGH-C210</td>
<td>SGH-C225</td>
<td>SGH-C230</td>
<td>SGH-C240</td>
<td>SGH-C250</td>
<td>SGH-C260</td>
</tr>
<tr>
<td>SGH-C300</td>
<td>SGH-C520</td>
<td>SGH-D307</td>
<td>SGH-D357</td>
<td>SGH-D410</td>
<td>SGH-D415</td>
</tr>
<tr>
<td>SGH-D488</td>
<td>SGH-D500</td>
<td>SGH-D500E</td>
<td>SGH-D510</td>
<td>SGH-D520</td>
<td>SGH-D550</td>
</tr>
<tr>
<td>SGH-D600</td>
<td>SGH-D700</td>
<td>SGH-D710</td>
<td>SGH-D720</td>
<td>SGH-D730</td>
<td>SGH-D800</td>
</tr>
<tr>
<td>SGH-D820</td>
<td>SGH-D830</td>
<td>SGH-D840</td>
<td>SGH-D880</td>
<td>SGH-D900</td>
<td>SGH-D900i</td>
</tr>
<tr>
<td>SGH-E105</td>
<td>SGH-E200</td>
<td>SGH-E250</td>
<td>SGH-E300</td>
<td>SGH-E310</td>
<td>SGH-E315</td>
</tr>
<tr>
<td>SGH-E317</td>
<td>SGH-E335</td>
<td>SGH-E340</td>
<td>SGH-E360</td>
<td>SGH-E370</td>
<td>SGH-E380</td>
</tr>
<tr>
<td>SGH-E390</td>
<td>SGH-E410</td>
<td>SGH-E420</td>
<td>SGH-E480</td>
<td>SGH-E490</td>
<td>SGH-E500</td>
</tr>
<tr>
<td>SGH-E530</td>
<td>SGH-E570</td>
<td>SGH-E590</td>
<td>SGH-E600</td>
<td>SGH-E610</td>
<td>SGH-E620</td>
</tr>
<tr>
<td>SGH-E640</td>
<td>SGH-E710</td>
<td>SGH-E715</td>
<td>SGH-E720</td>
<td>SGH-E730</td>
<td>SGH-E740</td>
</tr>
<tr>
<td>SGH-E750</td>
<td>SGH-E760</td>
<td>SGH-E770</td>
<td>SGH-E780</td>
<td>SGH-E790</td>
<td>SGH-E810</td>
</tr>
<tr>
<td>SGH-E830</td>
<td>SGH-E840</td>
<td>SGH-E870</td>
<td>SGH-E900</td>
<td>SGH-E910</td>
<td>SGH-E950</td>
</tr>
<tr>
<td>SGH-F300</td>
<td>SGH-F490</td>
<td>SGH-F500</td>
<td>SGH-G600</td>
<td>SGH-G800</td>
<td>SGH-G810</td>
</tr>
<tr>
<td>SGH-I250</td>
<td>SGH-I300</td>
<td>SGH-I500</td>
<td>SGH-I505</td>
<td>SGH-I530</td>
<td>SGH-I550</td>
</tr>
<tr>
<td>SGH-I700</td>
<td>SGH-I750</td>
<td>SGH-I600E</td>
<td>SGH-I-M300</td>
<td>SGH-I-P207</td>
<td>SGH-I-P310</td>
</tr>
<tr>
<td>SGH-P400</td>
<td>SGH-P410</td>
<td>SGH-P510</td>
<td>SGH-P705</td>
<td>SGH-P710</td>
<td>SGH-P738</td>
</tr>
<tr>
<td>SGH-P738</td>
<td>SGH-P850</td>
<td>SGH-P860</td>
<td>SGH-I-U100</td>
<td>SGH-I-U300</td>
<td>SGH-I-U600</td>
</tr>
<tr>
<td>SGH-U700</td>
<td>SGH-I-U900</td>
<td>SGH-X160</td>
<td>SGH-X200</td>
<td>SGH-X300</td>
<td>SGH-X450</td>
</tr>
<tr>
<td>SGH-X548</td>
<td>SGH-X475</td>
<td>SGH-X480</td>
<td>SGH-X510</td>
<td>SGH-X520</td>
<td>SGH-X530</td>
</tr>
<tr>
<td>SGH-X540</td>
<td>SGH-X620</td>
<td>SGH-X630</td>
<td>SGH-X640</td>
<td>SGH-X650</td>
<td>SGH-X660</td>
</tr>
<tr>
<td>SGH-X670</td>
<td>SGH-X680</td>
<td>SGH-X700</td>
<td>SGH-X800</td>
<td>SGH-X810</td>
<td>SGH-X820</td>
</tr>
<tr>
<td>SGH-Z100</td>
<td>SGH-Z105</td>
<td>SGH-Z107</td>
<td>SGH-Z130</td>
<td>SGH-Z300</td>
<td>SGH-Z500</td>
</tr>
<tr>
<td>SGH-Z540</td>
<td>SPH-A900</td>
<td>SPH-A920</td>
<td>SPH-A900</td>
<td>SPH-A920</td>
<td>SPH-A920</td>
</tr>
</tbody>
</table>
Table 6. Manufacturer: SonyEricsson. Models:

<table>
<thead>
<tr>
<th>C902</th>
<th>D750i</th>
<th>F500i</th>
<th>G502</th>
<th>J300</th>
<th>J300i</th>
</tr>
</thead>
<tbody>
<tr>
<td>K300</td>
<td>K3O0a</td>
<td>K300i</td>
<td>K310a</td>
<td>K310c</td>
<td>K310i</td>
</tr>
<tr>
<td>K320i</td>
<td>K500</td>
<td>K500c</td>
<td>K500i</td>
<td>K508i</td>
<td>K510a</td>
</tr>
<tr>
<td>K510c</td>
<td>K510i</td>
<td>K550c</td>
<td>K550i</td>
<td>K550im</td>
<td>K600i</td>
</tr>
<tr>
<td>K608i</td>
<td>K610i</td>
<td>K610im</td>
<td>K618i</td>
<td>K700i</td>
<td>K750c</td>
</tr>
<tr>
<td>K750i</td>
<td>K758c</td>
<td>K770i</td>
<td>K790a</td>
<td>K790c</td>
<td>K790i</td>
</tr>
<tr>
<td>K800i</td>
<td>K810i</td>
<td>K818c</td>
<td>K850i</td>
<td>M600i</td>
<td>M608c</td>
</tr>
<tr>
<td>P1c</td>
<td>S500c</td>
<td>P900</td>
<td>P910</td>
<td>P990c</td>
<td>P990i</td>
</tr>
<tr>
<td>S710a</td>
<td>V600</td>
<td>V600i</td>
<td>V630i</td>
<td>V640i</td>
<td>V800</td>
</tr>
<tr>
<td>V802SE</td>
<td>W200a</td>
<td>W200c</td>
<td>W200i</td>
<td>W300c</td>
<td>W300i</td>
</tr>
<tr>
<td>W550c</td>
<td>W550i</td>
<td>W580c</td>
<td>W580i</td>
<td>W600i</td>
<td>W600c</td>
</tr>
<tr>
<td>W600i</td>
<td>W610c</td>
<td>W610i</td>
<td>W660i</td>
<td>W700i</td>
<td>W710c</td>
</tr>
<tr>
<td>W710i</td>
<td>W712a</td>
<td>W800c</td>
<td>W800i</td>
<td>W810c</td>
<td>W810i</td>
</tr>
<tr>
<td>W830c</td>
<td>W830i</td>
<td>W850i</td>
<td>W880i</td>
<td>W880iv</td>
<td>W888c</td>
</tr>
<tr>
<td>W900c</td>
<td>W900i</td>
<td>W908c</td>
<td>W910i</td>
<td>W950c</td>
<td>W950i</td>
</tr>
<tr>
<td>W958c</td>
<td>Z1010</td>
<td>Z200</td>
<td>Z320a</td>
<td>Z320c</td>
<td>Z320i</td>
</tr>
<tr>
<td>Z500</td>
<td>Z520a</td>
<td>Z520c</td>
<td>Z520i</td>
<td>Z525a</td>
<td>Z525i</td>
</tr>
<tr>
<td>Z530c</td>
<td>Z530i</td>
<td>Z550c</td>
<td>Z550i</td>
<td>Z550i</td>
<td>Z610i</td>
</tr>
<tr>
<td>Z710c</td>
<td>Z710i</td>
<td>Z750i</td>
<td>Z800</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
15. Main priorities

The original programs are protected by state registration certificates:

- “Check-In-Phone Mobile container + Wallet (the one unit)” (the “Wallet”). The mobile Application in a mobile phone. The state registration certificate of the informational system program № 2008613820 dated 11 August 2008.

- “Check-In-Phone AuthenticGate” (“CIP_AG”). Front-end server Application (Authentication System). The state registration certificate of the informational system program № 2008613819 dated 11 August 2008.


- “Check-In-Phone Access Point” (“CIP_AP”). The gateway to the server Application of the Partner. The state registration certificate of the informational system program № 2008614383 dated 11 September 2008.
16. Persons

Goldovkiy Igor. The leading specialist involved in area of plastic cards, the author of two monographs on chip cards and electronic commerce. For many years, he was General Director for “STB CARD” which was the largest card processing company in Russia. Ideologist and inspirer of the project, the experienced organizer and ideological locomotive. Education obtained - Moscow Institute of Physics and Technology, PhD (Dr. of Physics and Mathematics).

Kuznetsov Andrew. The experienced specialist in the field of the secured Applications development for SIM cards and mobile phones, has managed the projects on banking Applications realization on SIM cards of MBRR, Sberbank and some other banks, developed the Applications for SIM-cards mobile operators (MEGAFON, MTS). Education obtained- Moscow State Institute of Electronics and Mathematics.

Soloviev Evgeny. The specialist involved in company developing. The author of the number of the articles on technology of organizing the business-processes in banking cards field, has the 15 years experience in banking cards industry. “STBCARD” company executive director. Education obtained - Moscow State University (Mathematics).
17. Banking details

The system procurement, implementation, integration and maintenance:

The Mobile Solutions Co Ltd
INN/KPP 7743683060/7744301001
Address: Russian Federation 125445 Moscow, Smolnaya Str., 22
Settlement account № 407028105000000020072
in VTB24 (ZAO) Bank
Corresponding account 30101810100000000716
in OPERU MGTS Bank of Russia
BIC 044525716
INN 7710353606
OKPO 85669012
OKVD 72.1
## 18. The services components

<table>
<thead>
<tr>
<th>Phases and milestone events</th>
<th>The executive</th>
<th>Unit man-hours</th>
<th>Terms, working days</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project preliminary arrangements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BRD agreement</td>
<td></td>
<td>MS</td>
<td></td>
</tr>
<tr>
<td>Preparing of the implementation project, specifications, requirement specifications,</td>
<td></td>
<td>MS</td>
<td></td>
</tr>
<tr>
<td>for system integration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Procuring and implementation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License and service agreements concluding</td>
<td></td>
<td>MS</td>
<td></td>
</tr>
<tr>
<td>Base installation and software programs setting up</td>
<td></td>
<td>MS</td>
<td></td>
</tr>
<tr>
<td>Mobile Application designing</td>
<td></td>
<td>MS</td>
<td></td>
</tr>
<tr>
<td>Carrying out modifications pursuant to requirement specifications (required to be defined)</td>
<td></td>
<td>MS</td>
<td></td>
</tr>
<tr>
<td>Integration with the informational system (required to be defined)</td>
<td></td>
<td>MS</td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
<td>MS</td>
<td></td>
</tr>
<tr>
<td>Project management</td>
<td></td>
<td>MS</td>
<td></td>
</tr>
</tbody>
</table>
19. **The licenses procured with the solutions**

<table>
<thead>
<tr>
<th>Program solutions</th>
<th>Number of licenses, units</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ApplicWard</strong></td>
<td></td>
</tr>
<tr>
<td>The server Application for elaborating and managing the mobile Applications at mobile phones: personal data receiving, mobile Applications personification, uploading to mobile phones, cryptographic data management and etc. The number of the processed Applications isn’t limited.</td>
<td>1</td>
</tr>
<tr>
<td><strong>Authentic Gate</strong></td>
<td></td>
</tr>
<tr>
<td>Server Application for Users authentication from mobile phones, for supporting interface with the access point</td>
<td>1</td>
</tr>
<tr>
<td><strong>Access point</strong></td>
<td></td>
</tr>
<tr>
<td>Server interface Application to communicate with the customer’s systems ApplicWard and Authentic Gate. The number of interfaces with the systems of the Customer isn’t limited</td>
<td>1</td>
</tr>
<tr>
<td><strong>Cryptoserver</strong></td>
<td></td>
</tr>
<tr>
<td>Server Application meant for cryptographic transactions carrying out</td>
<td>1</td>
</tr>
<tr>
<td><strong>The renewed telephone database</strong></td>
<td></td>
</tr>
<tr>
<td>Server Application: the database for supporting Applications uploaded to mobile phones</td>
<td>1</td>
</tr>
<tr>
<td><strong>Check-In-Phone</strong></td>
<td></td>
</tr>
<tr>
<td>Client’s Application at the User’s mobile phone</td>
<td>N</td>
</tr>
</tbody>
</table>
## 20. Software

System software specifications

| System equipment | 1) Web-server  
2) Applications server (CIP ApplicWard, CIP Authentic Gate)  
3) Cryptoserver  
4) Database server ORACLE, MySQL Server 5  
5) System operator working station |
|------------------|---------------------------------------------------------------|
| Web-server:      | o OS Unix (Sun Solaris 10 SPARC), Linux, Windows  
                   o Apache HTTP Server 2.2.10 |
| Applications server: | o OS Unix (Sun Solaris 10 SPARC), Linux, Windows  
                                   o Sun Java Application Server 9.1-02  
                                   o JDK version not less that 1.5_09  
                                   o Subversion 1.4.5 |
| Cryptoserver:    | o OS Unix (Sun Solaris 10 SPARC), Linux, Windows  
                   o Sun Java Application Server 9.1-02  
                   o JDK version not less that 1.5_09  
                   o Subversion 1.4.5 |
| Database server: | o OS Unix (Sun Solaris 10 SPARC), Linux, Windows  
                   o Database Oracle, MySQL Server 5 |
The overall scheme of the central hardware/software platform is described below.

Central server equipment specifications (option):

1. The equipment in a rack:

1.1. Sun Fire Server V215 (Web server):
   - Processor model, the number of processors 1x Sun UltraSPARC IIIi
   - RAM volume 4096 MB
   - Type, volume and number of HDD 2x 73 GB SAS 2.5-inch disk
   - Height RACK/1U
   - EPU number and power 2x320 W
   - Type and the number of optical storage device - no
   - Number of network cards 4
   - Additional components ALOM Remote Manager

1.2. Sun Netra Server X4200 M2 (Applications Server):
   - Processor model, the number of processors 1x Dual core Next Generation AMD
   - RAM volume 8048 MB
   - Type, volume and number of HDD 2x 73 GB SAS 2.5-inch disk
   - Height RACK/2U
   - EPU number and power 2x230 W
1. The type and the number of optical storage device 1xDVD/CD-RW
2. Number of network cards 4+1

1.3. **Sun Netra Server X4200 M2 (CryptoServer/Database Server)**
   - Processor model, the number of processors 1x Dual core Next Generation AMD
   - RAM volume of 8048 MB
   - Type, volume and number of HDD 2x 73 GB SAS 2.5-inch disk
   - Height RACK/2U
   - EPU number and power 2x230 W
   - Type and the number of optical storage device 1xDVD/CD-RW
   - Number of network cards 4+1
   - Additional components: HSM Eracom ProtectServer Gold

1.4. **Firewall Check Point UTM-1 EDGE X**
   - Height Rack/1U

Server equipment specifications of the for Check-In-Phone Access Point is below (option):
   - Processor Intel Xeon Quad-frequency from 2 GHz and higher (for instance, HP ProLiant ML 150 G5 Intel Xeon E5405 2 GHz. RAM- from 2GHz and higher.
   - Slot PCI-X for HSM connection (mandatory) (Eracom ProtectServer Gold, Orange)
   - Hard disks of SAS standard (1-2 discs with the volume 73, 4 GB each)
   - UPS
   - HSM (Eracom ProtectServer Gold or Orange)