

BANKING, INSURANCE & CAPITAL MARKETS

Authentication and authorization on mobile devices

Comarch Mobile Security



COMARCH
INFORMATION TECHNOLOGY

2

Introduction

User authentication and authorization represent key elements in IT system security. Authentication confirms user identities, while authorization grants users access according to specific security principles and also allows them to confirm the credibility of transactions. Authentication is the first line of defense against unauthorized access.

The authentication process can be conducted in many ways. First of all there is the simple defense afforded by static passwords. Next, there are one-time passwords generated by tokens. Finally, there are certificates loaded on to smart (cryptographic) cards and biometric readers.

To overcome these challenges, we have created a new authentication and authorization method based on mobile phones that combines features never before seen together in one solution. It delivers security, ease of use and advanced technology at a low price.

Comarch MobileID

Comarch MobileID is a low cost solution that delivers high security and transferability to the end user.

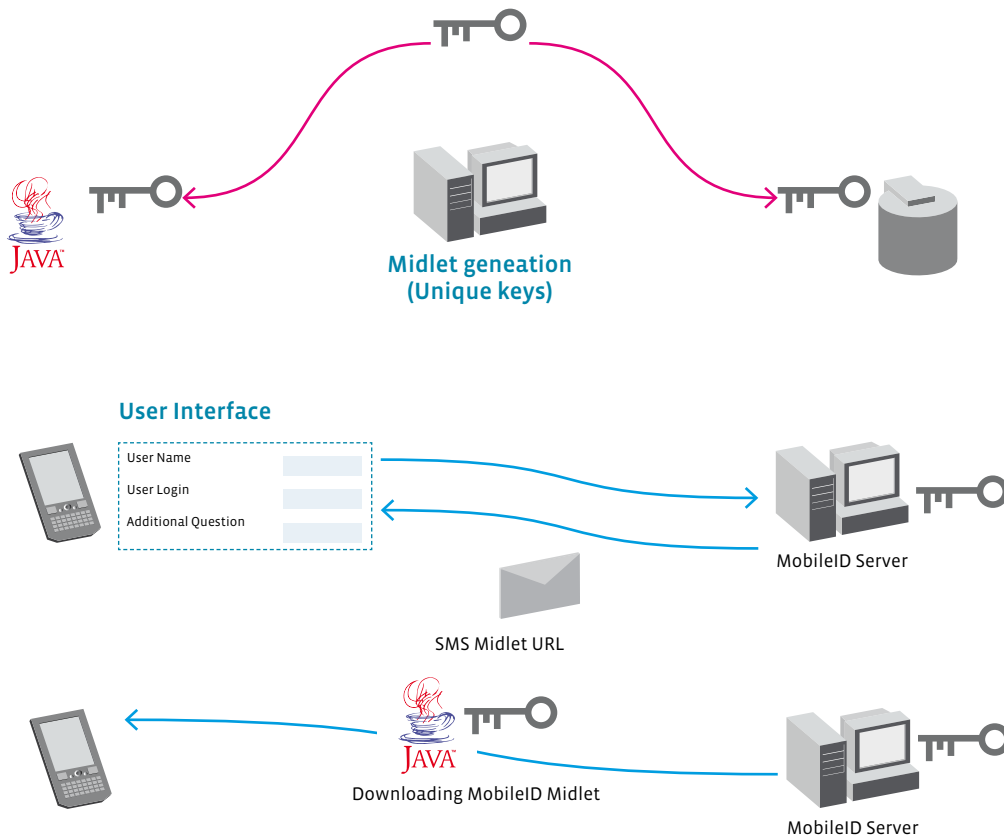
Simple Installation

The user registers in the system by giving a user name. He is also asked for a mobile phone number. The server automatically sends a download link for Comarch MobileID to this number. This distribution method is extremely easy and convenient for the end user.

During the registration process individual cryptographic keys are being generated for the user (they are also stored in MobileID database). Also the midlet is being created and it is ready to download by the end user.

After the registration the user receives a password, which is used to authenticate during the download of MobileID application. He also receives the first PIN to the application, which can be changed anytime with the aid of the server component's user interface. The address, from which the application should be downloaded, is being sent to the end user through SMS.

After opening the message the user is immediately being connected with the server, from which the MobileID midlet is to be downloaded. This midlet contains user's individual keys.



Downloading MobileID Midlet

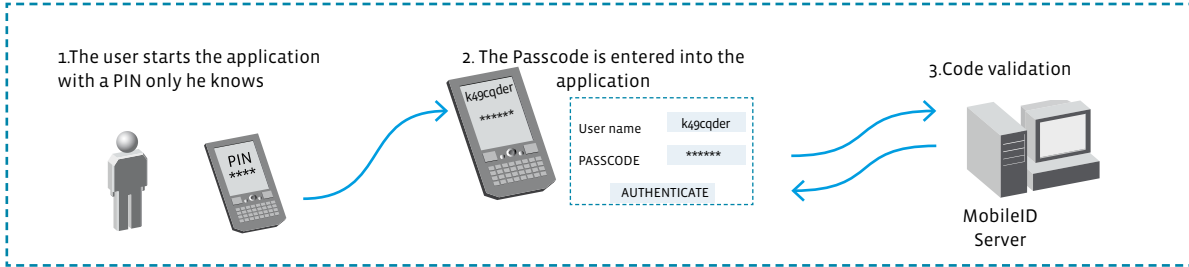
4

Authentication

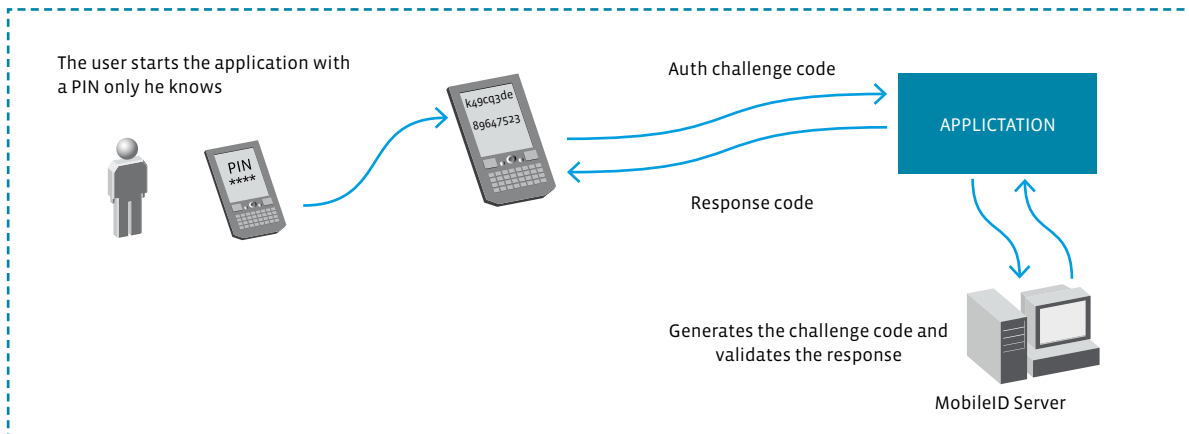
During the login process the user is being asked by the application to provide his login name and PASSCODE generated by Comarch MobileID. In order to do that he has to launch the application on his mobile phone initiating it with PIN known only to him.

The application generates the PASSCODE by which the user confirms his identity.

A two-part authentication takes place involving what the user knows (PIN) and what the user possesses – a mobile device with a personalized Comarch MobileID.



User Authentication with Comarch MobileID

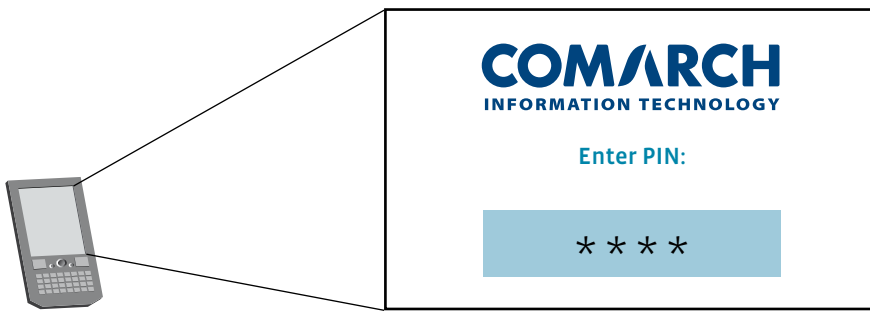


Transaction Authorization with Comarch MobileID

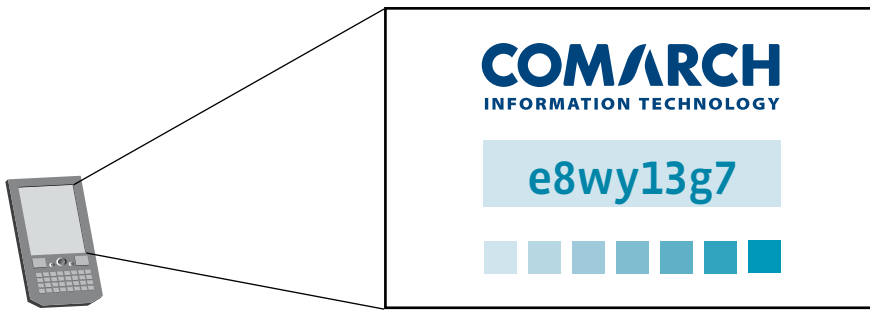
Transaction Authorization

Transaction authorization is a two-stage process: the server generates a Challenge code, which the user enters into Comarch MobileID. This is used to generate the

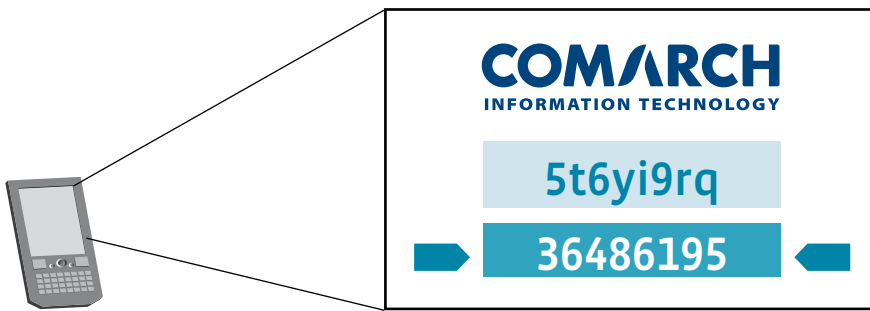
appropriate authorization Response code. The Challenge code includes data on the transaction thus increasing security.



Comarch Mobile ID Start-up – User PIN Entry Mode



Comarch Mobile ID – User Authorization Mode



Comarch MobileID: Transaction Authorization Mode

6

Personalization of the solution

Comarch MobileID can be customized according to the customer’s wishes.

Below are some example screen dumps from personalized Comarch MobileID applications. The first shows the login screen for the Comarch MobileID application: enter PIN. The second features Comarch MobileID in authentication mode: generate PASSCODE. The third is a view of Comarch MobileID in transaction authorization mode: generate *challenge-response* token.

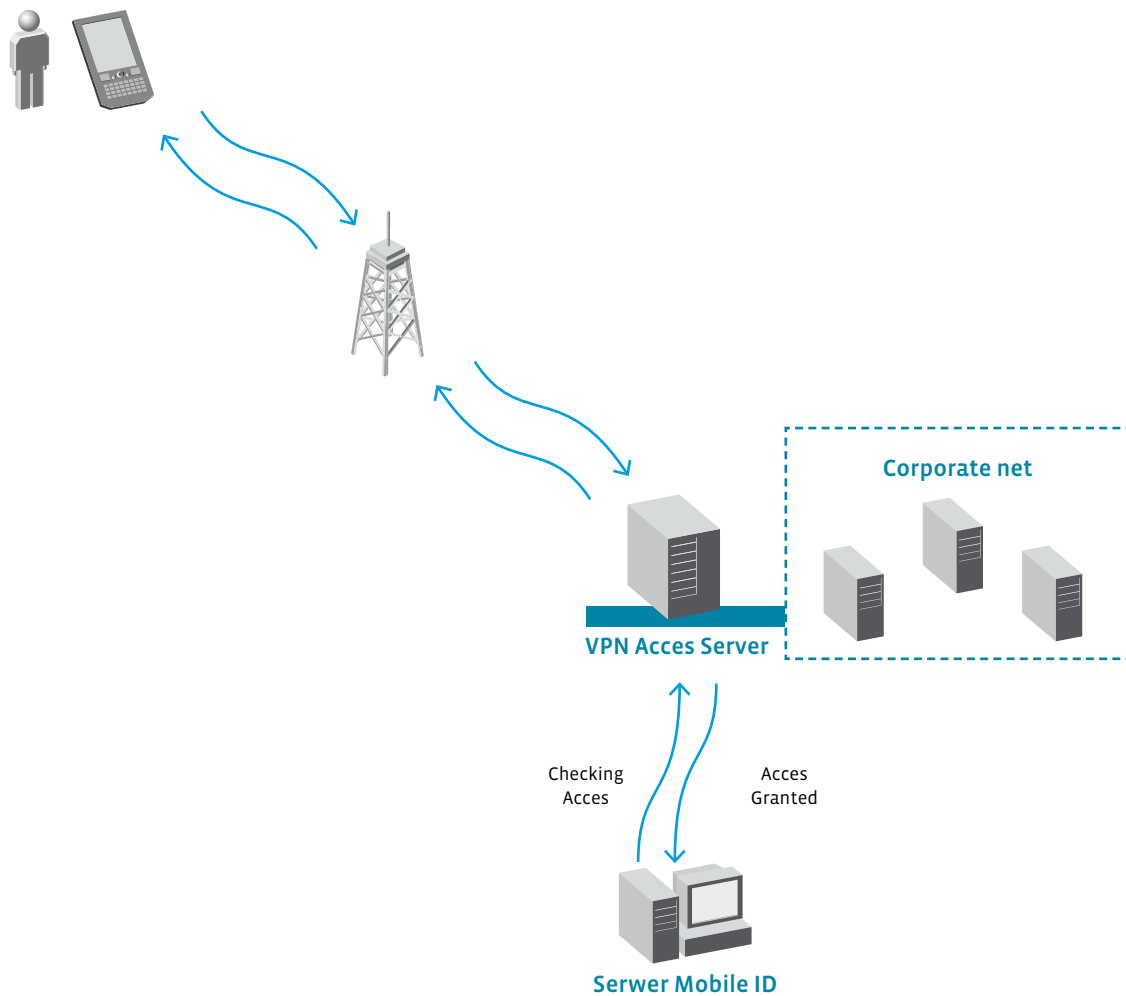
Radius protocol attendance

The most popular user access authentication and authorization protocol for network users:

- Dial-up networks
- Wireless network (802.X protocol)
- Tunnels (VPN)

It is widely used for VoIP access (SIP and H.323).

Comarch MobileID integrates easily with Radius servers giving the user additional options for access to the networks and services described above. Instead of the stan-



Comarch MobileID: Interaction with Devices using Radius Protocol

standard authorization and authentication protocols such as PAP, CHAP and others of the user/password type, the user can login with Comarch MobileID making access much easier and providing enhanced security.

Features

Strong Cryptography:

cryptographically secure pseudorandom number generator,

symmetric algorithms: AES (Advanced Encryption Standard),

hash functions: **SHA256**,

Two-part authentication and authorization:

- what the user knows (PIN)
- what the user possesses – a mobile device with a Comarch MobileID midlet
- Passcode generated every sixty seconds,
- Passcode can only be used once.

Other features:

- Radius protocol attendance,
- low costs: no requirement for additional devices and no costs arising from sending SMSs,
- Comarch MobileID user interface individually customized for the customer,
- easy to install.

Served Devices

Every mobile phone with MIDP 1.0 attendance – nearly every one produced after 2002.

Comarch MobilePKI

Making creative use of new techniques and technologies Comarch has developed **Comarch MobilePKI** which enables full use of public key infrastructure on mobile phones with SIM cards.

Simple Installatio

Comarch MobilePKI authentication and authorization is based on a java application installed on a SIM card (with the full option with cryptoprocessor). The application converts the mobile phone into a cryptographic card that contains a public and private key and does not require a card reader for signature submission. SMSs are used to communicate with the transaction system for key generation, activation and signature submission.

Using this authentication and authorization method requires no additional mobile phone operator services. The only change required is to substitute the common SIM card for a SIM with a crypto-processor. It is also possible to come to an agreement with the mobile phone operator to add Comarch MobileID to the SIM card.

There are two ways to upload the Comarch MobilePKI application:

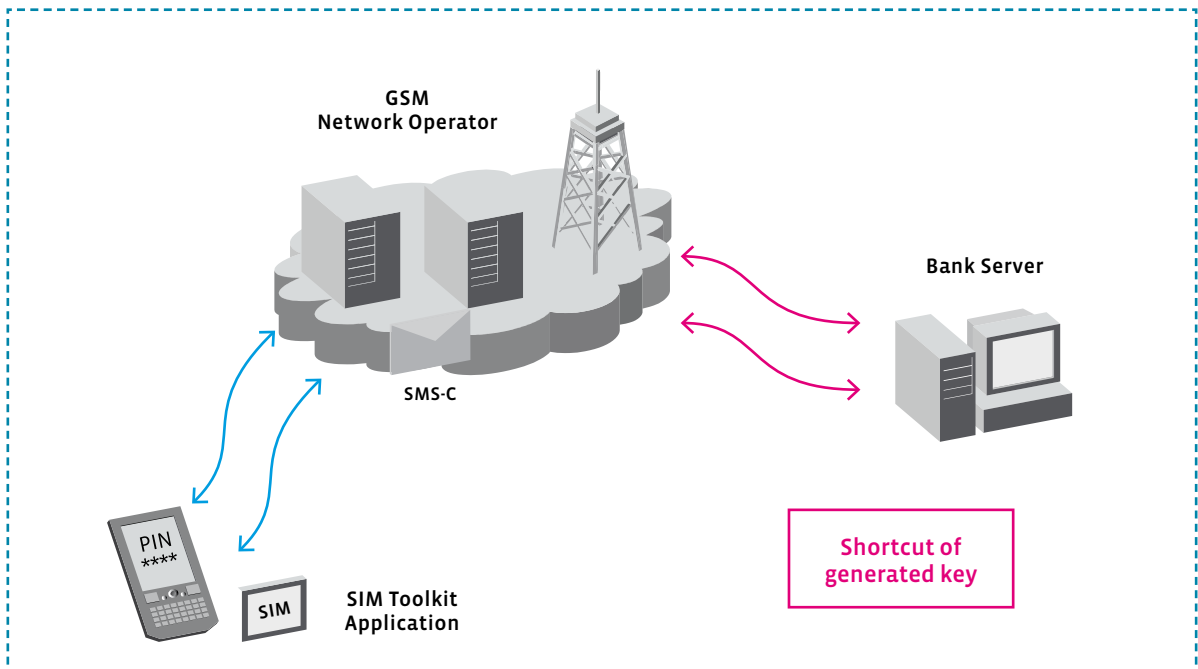
- at the bank's place of business
- at the seat of a mobile phone operator

In both cases the employee puts the SIM card from the customer's phone into a SIM card reader and uploads the application.

Key Generation / Activation

The Comarch MobilePKI application communicates with the bank's transaction system by automatically reacting to a specific SMS. The keys (private and public) are generated by incoming SMSs. A public key is returned to the transaction system. This is used by the integrated transaction system to check the signature and authorization for the transaction.

Comarch MobilePKI has additional security installed for key transactions. The newly generated key has to be activated for the authentication and authorization system to work. One activation path involves the end



Comarch MobilePKI: Authorization and Authentication

user phoning the bank's information line and having the bank employee send the activating SMS from the transaction system. Of course, depending on the specific implementation concerned, the user can activate the key himself.

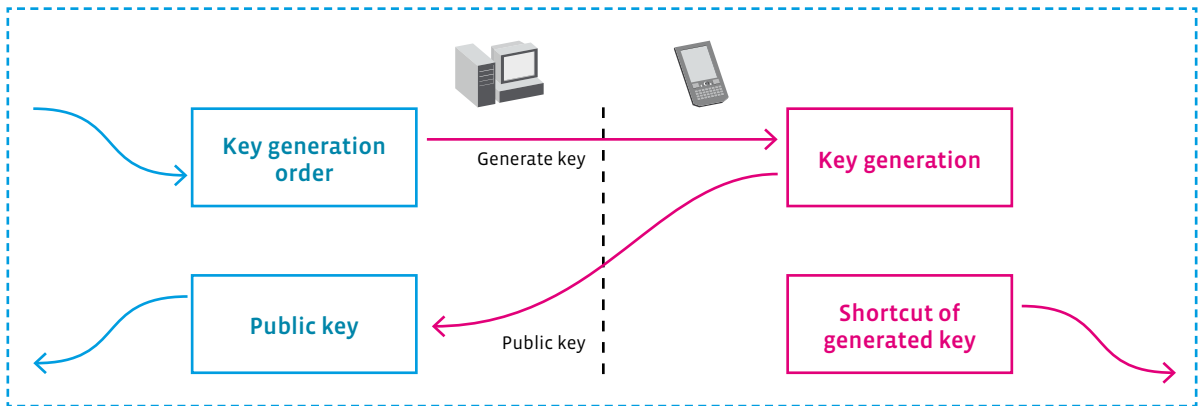
Transaction Authorization

Authorization for single transactions – the bank's transaction system sends an SMS to the user's mobile phone and this message is automatically detected by the Comarch MobilePKI application. The phone's screen then displays the information that the transaction is ready to be authorized, that is, to be signed with the user's private key. The transaction details are then displayed to the user for verification. The electronic

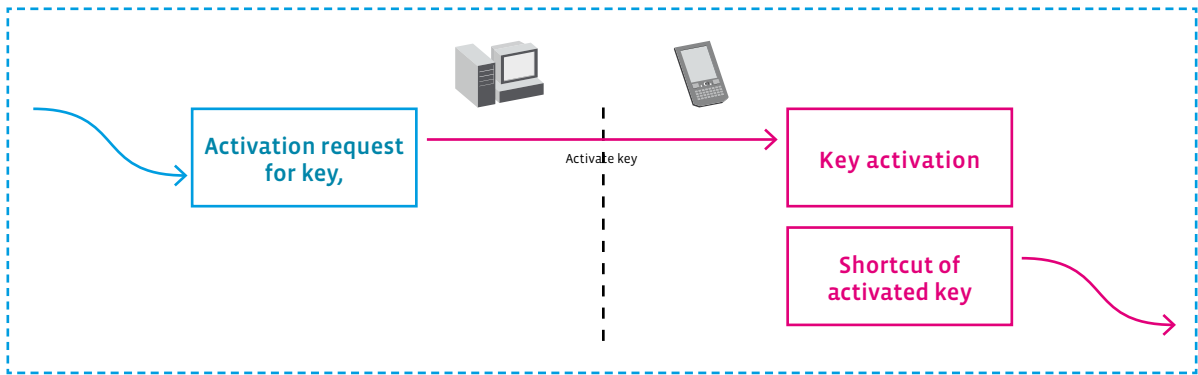
signature (the shortcut to the information encrypted in the private key) is returned by SMS to the transaction system which verifies the signature by reference to the private key.

Batch authorizations – when the bank's transaction system prepares a batch of transfers (information) for signing, an SMS is sent containing the batch's checksum, data about the batch and the total value of the transfer. Once the SMS has been received the batch is signed and the electronic signature itself is returned to the bank's transaction system via SMS.

Where batch authorization is treated as a set of individual transactions, that is, where signing is required for



Key Generation



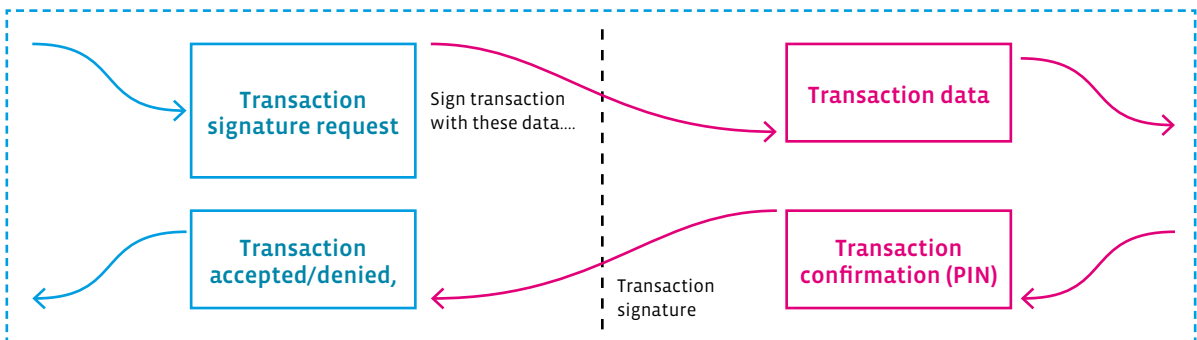
Key Activation

each discrete transaction in the batch, an exchange of SMSs is necessary for each of them.

System Features

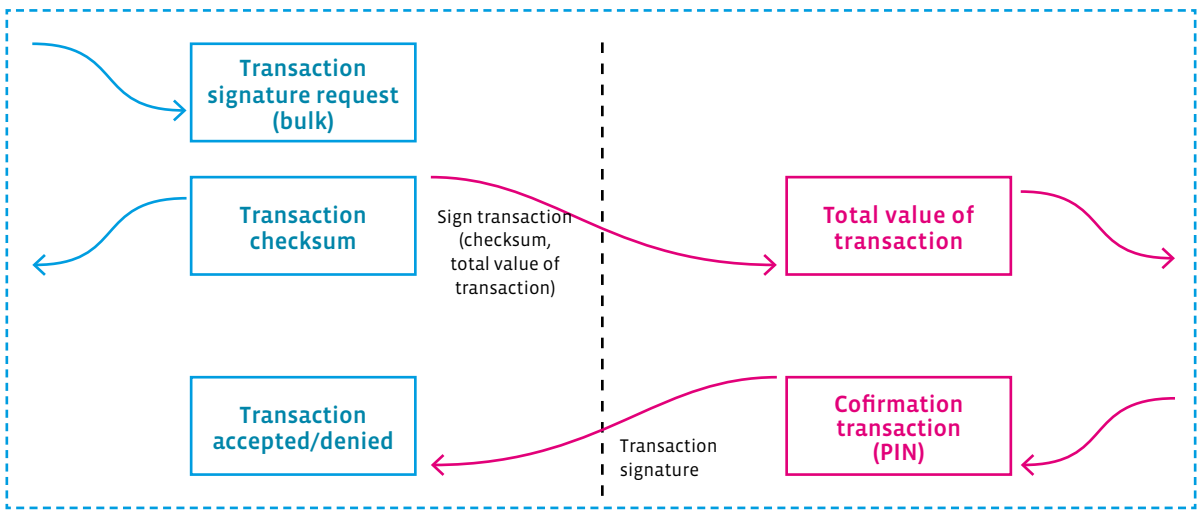
- telephone – bank (transaction system) communication by SMS,
- compatible with STK GSM 11.14 standard,
- uses RSA 1024 bit keys,

- keys generated by an application on a SIM card (in the case of cryptographic cards on the card),
- supports use of multiple key pairs,
- private key protected by PIN,
- SIM cards can be unblocked by SMS,
- easy installation.



Authorization for single transaction

10



Batch Authorization

Devices and Equipment Supported

The Comarch MobilePKI application works on SIM cards in accordance with JavaCard specifications 2.1.1/2.2.1

Full implementation of Comarch MobilePKI requires a SIM card with a cryptoprocessor - in order to make impossible to remove a private key from a SIM card re-

quired is a cryptographic card. Private key generation then takes place on a SIM card, access to the card is secured and the key cannot be extracted.

Comarch Headquarters

Al. Jana Pawła II 39 a
31-864 Krakow
Poland

phone: +48 12 64 61 000

fax: +48 12 64 61 100

e-mail: info@comarch.pl

Comarch Inc.

10 W 35th Street
Chicago, IL 60616
United States

phone: +1 800 786 4408

fax: +1 800 684 5916

e-mail: info@comarch.com

Comarch Software AG

Chemnitzer Str. 50
01187 Dresden
Germany

phone: +49 351 3201 3200

fax: +49 351 438 97 10

e-mail: info@comarch.de

Comarch OOO

Prechistenskiy Pereulok 14/1
119034 Moscow
Russia

phone: +7 495 783 36 71

Poland

Gdansk, Katowice Krakow,
Lublin, Lodz, Poznan,
Szczecin, Warsaw, Wroclaw

Belgium Brussels

France Lille

Germany Dresden,
Frankfurt/Main

Lithuania Vilnius

Panama Panama City

Russia Moscow

UAE Dubai

Ukraine Kiev, Lviv

USA Chicago, Miami

www.finance.comarch.com

www.comarch.com www.comarch.pl www.comarch.de www.comarch.ru

Comarch is a leading Central European IT business solutions provider specializing in forging business relationships that maximize customer profitability while optimizing business and operational processes. Comarch's primary advantage lies in the vast domain of knowledge accumulated in and applied to our software products. These products incorporate highly sophisticated IT solutions for businesses in all vertical sectors. Comarch has a multinational network of offices employing over 2800 highly-experienced IT specialists in Europe, the Middle East and the Americas.

ComArch Spółka Akcyjna with its registered seat in Kraków at Aleja Jana Pawła II 39A, entered in the National Court Register kept by the District Court for Kraków-Sródmieście in Kraków, the 11th Commercial Division of the National Court Register under no. KRS 000057567. The share capital amounts to 7,960,596.00 zł. The share capital was fully paid, NIP 677-00-65-406

Copyright © Comarch 2008. All Rights Reserved. No part of this document may be reproduced in any form without the prior written consent of Comarch. Comarch reserves the right to revise this document and to make changes in the content from time to time without notice. Comarch may make improvements and/or changes to the product(s) and/or programs described in this document any time. The trademarks and service marks of Comarch are the exclusive property of Comarch, and may not be used without permission. All other marks are the property of their respective owners.

COMARCH