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.

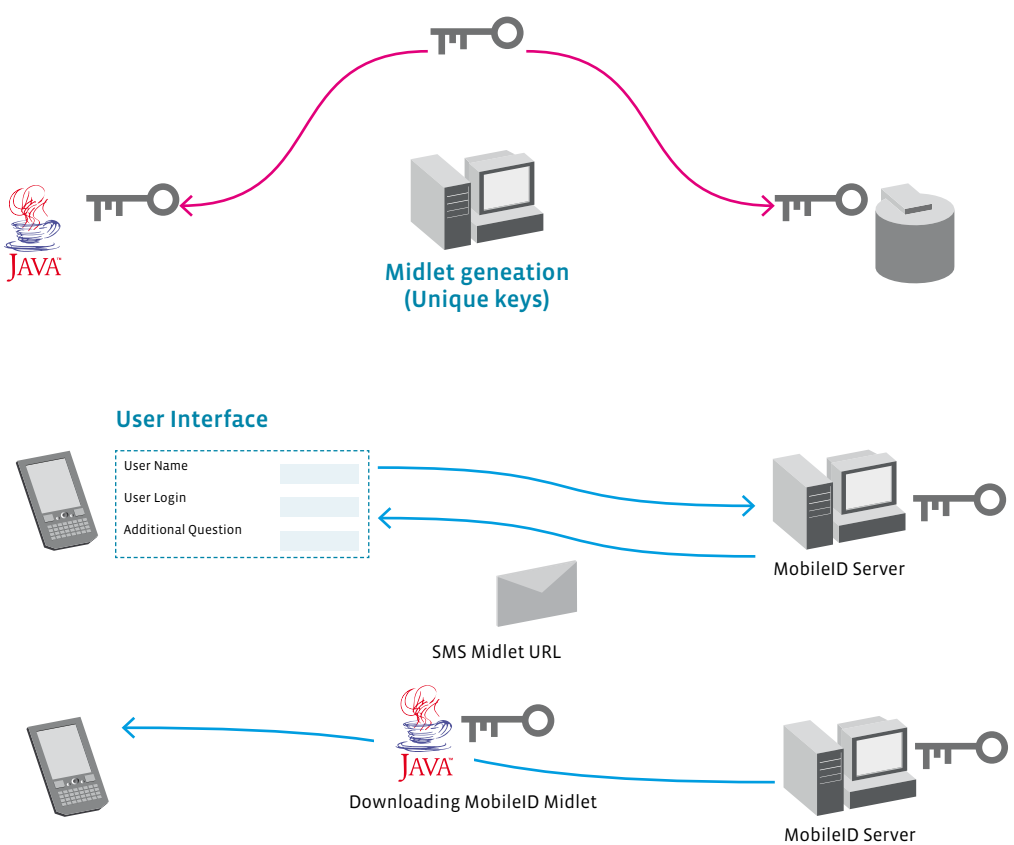
Simple Installation

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

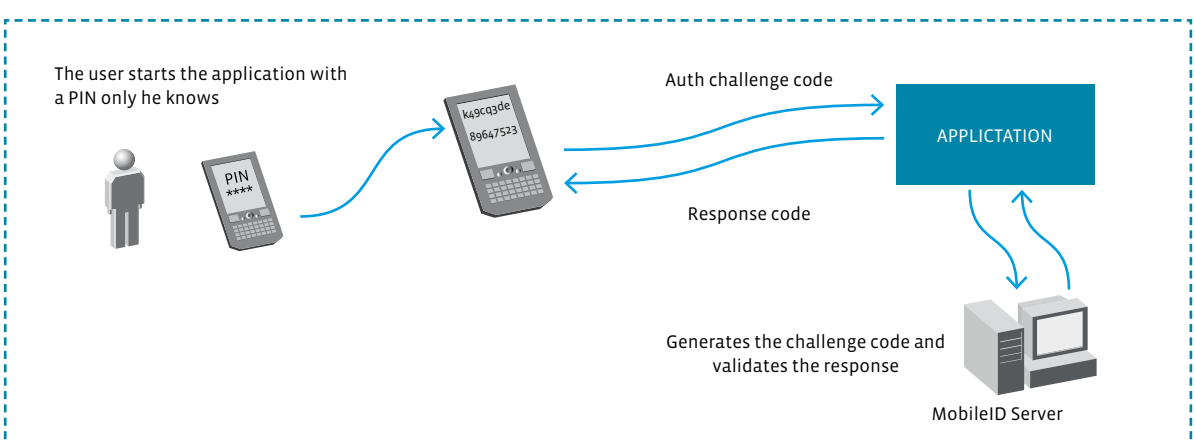
Authentication

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.

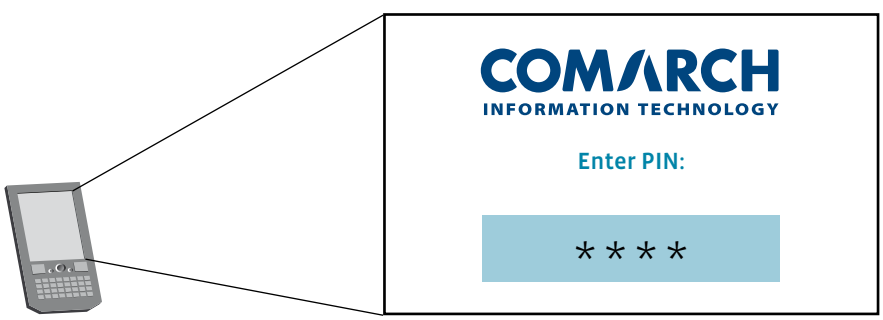
User Authentication with Comarch MobileID



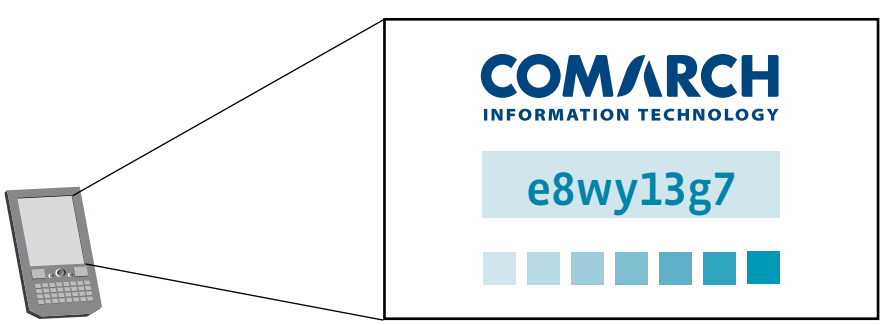
Transaction Authorization with Comarch MobileID

Transaction Authorization

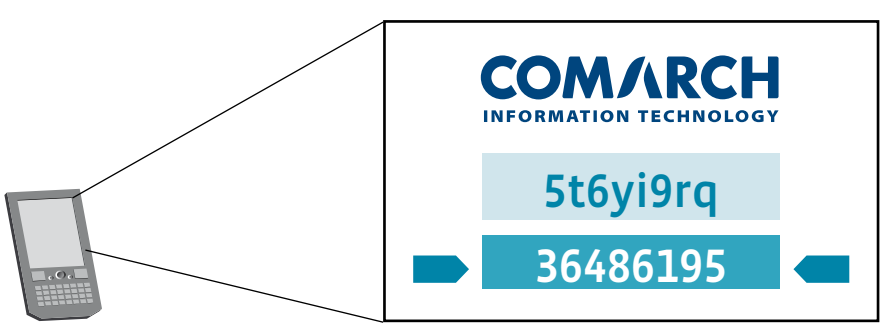
Transaction authorization is a two-stage process: the server generates a Challenge code, which the user enters into Comarch MobileID. This is used to generate the appropriate authorization Response code. The Challenge code includes data on the transaction thus increasing security.



Comarch Mobile ID Start-up – User PIN Entry Mode



Comarch Mobile ID – User Authorization Mode



Comarch MobileID: Transaction Authorization Mode

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.

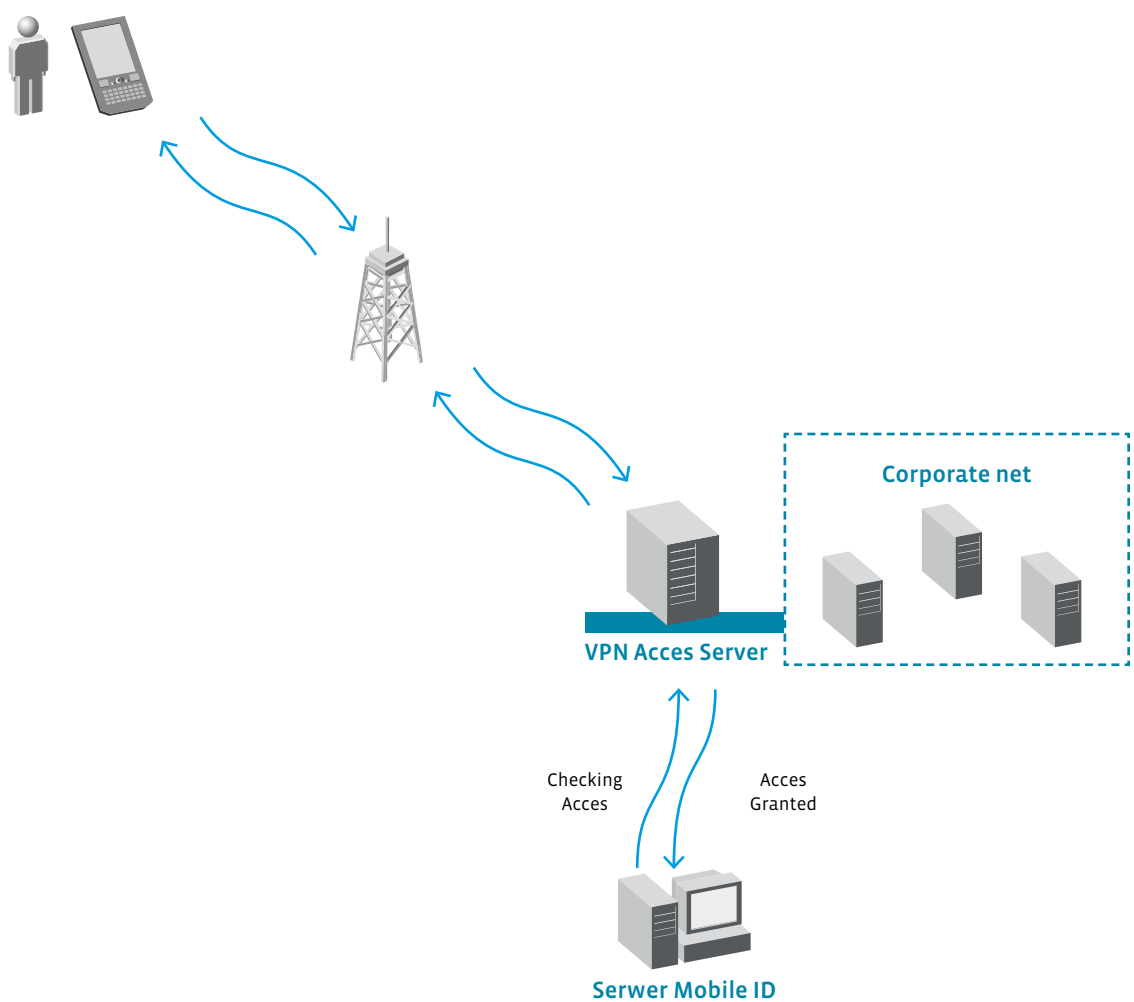
Radius protocol attendance

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

dard 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.