Millenet – Internet Banking
For Companies

User Instructions (part I)

February 12th, 2010
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.9.1 Initial Configuration</td>
<td>42</td>
</tr>
<tr>
<td>2.9.1.1 Initial Configuration with two Users</td>
<td>42</td>
</tr>
<tr>
<td>2.9.2 Small Business</td>
<td>43</td>
</tr>
<tr>
<td>2.9.2.1 Owner</td>
<td>43</td>
</tr>
<tr>
<td>2.9.2.2 Owner + Assistant</td>
<td>44</td>
</tr>
<tr>
<td>2.9.2.3 Two Co-owners + Assistant</td>
<td>45</td>
</tr>
<tr>
<td>2.9.3 Bigger Structure</td>
<td>46</td>
</tr>
</tbody>
</table>
Dear Client,

Thank you for joining the users of the Millenet Internet Banking System.

The Millenet system was created with a view to your convenience and effective management of your Company’s finances. The system is user friendly, which allows to quickly and safely carry out transfers, check the status of your Company’s assets and liabilities, as well as track detailed information relating to each operation. Additionally, in order to help you use the system, we prepared User Instructions.

Millenet provides you with services and information adjusted to your Company needs on a competitive market. Available services include among others opening deposits, ordering collective transfers, checking the current exchange rates at Bank Millennium, ordering documents electronically and many others.

Hopefully, using the Millenet system will give you much satisfaction and improve your Company’s operation.

We wish you many successful transactions.
1 General Information

The Millenet Internet Banking System was created to carry out financial operations connected with domestic and foreign settlements and depositing surplus funds. The system provides access to the following Client accounts at Bank Millennium S.A.: current accounts, term deposits, loans, guarantees, letters of credit and cards. It enables transfers between the Client’s own accounts and to counterparty accounts. Millenet also allows to monitor an operation and the process of its authorisation by particular Users, from the moment of its setting up in the system until its execution.

Millenet means:

- service availability on a 24/7 basis,
- mobility – access to accounts at Bank Millennium from each computer meeting the minimum technical and software requirements,
- no need to install additional software on the Client’s computer,
- lack of costs connected with additional licenses,
- possibility of carrying out a „multisignature” structure for executing transactions – up to three signatures,
- access to the system in the Polish and English language.

1.1 Technical Requirements and Hardware Settings

For setting up a correct Millenet System session you need a computer with access to the Internet and the browser Microsoft Internet Explorer 6.0 or newer, or Mozilla Firefox 1.0, or newer.

The most recent versions of the browsers are available free of charge from the Microsoft or Mozilla Foundation websites in the Download section (www.microsoft.com; www.mozilla.com). Moreover, the operational system and browsers must be regularly updated.

1.1.1 Settings of the Internet Explorer Browser

Select Tools on the upper bar of the browser menu, and then click Internet options:

- In the Security tab select the appropriate zone which is currently your location (Local Internet in this example) for each computer you use (e.g. at the office, at home, etc.), and then click Non-standard level:
in the **ActiveX Formants and plug-ins** group

- Select **Activate** with the **Initiating and executing ActiveX formant scripts not selected as secure (1)** option,

- select **Activate** with the option **Launching ActiveX Formants and Plug-ins (2)**,

- select **Activate** with the option **Executing ActiveX Formants as Secure (3)**,
in the **Script Service** group

- select **Activate** with the option **Executing Active Scripts (4)**,
In the Other group:
- **Switch off** with the option *Do not prompt the selection of the client certificate, if there are no certificates or just one exists* (5)

Then select the **Advanced** tab

In the **Security** group the following options should be selected:
- *Do not save coded pages on disk,*
- *Warn against invalid website certificates,*
- *Warn if sending of forms is being redirected,*
- *Check if the issuer’s certificate has been withdrawn*
- *Use SSL 3.0,*
- *Use TLS 1.0,*
Select the **General** tab to find **Temporary internet files**, click **Remove files (1)**, select **Remove all offline content (2)** and click **OK** to confirm (3).

Click **Settings** and then set the position **Every visit to the page (4)**. Select **OK (5)** and after you return to the **General** tab press **OK** to approve the Settings.

Close and reopen browser.
1.1.2 Settings of the Mozilla FireFox Browser

In the **Tools** menu from the upper browser bar select **Options**

![Mozilla FireFox Options Menu]

Then in **Advanced**, in the **Security** subgroup:
- select: **Use SSL 3.0**,
- select: **TSL 1.0**.

![Mozilla FireFox Advanced Security Options]

In the **Certificates** subgroup
- select **Ask every time**

![Mozilla FireFox Certificates Options]
Open **Web Features**:

- **Activate:** Enable **Java**,  
- **Activate:** Enable **JavaScript** and OK to confirm
1.2 Security

Millenet has the following security features:

- **SSL**—secured communication ensuring the most powerful **128-bit** data encryption,
- Double User logging with **MilleKod** and **Login**,
- Personal access **Password** for each of the Users with system privileges,
- SMS **P@sswords**, which are one-time codes texted to the mobile phone used for operation authorisations,
- Expanded user privileges management module,
- Registration module for all the Company’s operations executed via Millenet,
- Client authentication by means of Internet certificates which enable:
  - Strengthening data protection,
  - Creating secure network connections.

1.3 Rules of Security

1.3.1 Use Antivirus Software

Regrettably, it can sometimes happen that dangerous software - viruses or system intercepting programme – may appear in the system.

Good antivirus programmes regularly updated may help cure this type of problems and even prevent them. But even if a dangerous programme has been installed, then the antivirus programme can prevent its execution.

Never disable the antivirus programme! Several seconds will be enough to install spyware on your computer.

Antivirus on-line scanners include for example:
- Internet scanner Mks _vir
- Internet scanner ESET NOD32

Antivirus programmes include for example:
- Avast Home Edition
- ESET NOD32 Antivirus
- Norton AntiVirus
- Kaspersky Anti-Virus Personal
- Mks _vir

Some of the above-mentioned applications are freeware.
1.3.2 Use Personal Firewall

A personal firewall is a programme, which warns you when someone tries to remotely connect to your computer. It will also warn you when some programme from your computer tries to send information to someone from the outside network.

Using a personal firewall requires a more advanced understanding of the system installed on the computer in order to know which programmes should be allowed access to the network and which should be barred from it. But be smart to invest in knowing these things in order to hinder any attack whose purpose is to obtain access to confidential data.

This type of software includes:
- Sunbelt Personal Firewall
- Comodo Free Firewall
- Outpost Firewall Pro
- Kerio Winroute Firewall
- ZoneAlarm

Some of the above-mentioned applications are freeware.

1.3.3 Never respond to e-mails in which you are asked to provide confidential data!

The Bank never asks you to disclose any confidential data by electronic mail, so you should never answer e-mails in which you are asked to provide your confidential data such as:
- personal data,
- mother’s maiden name,
- bank account number,
- MilleKod,
- passwords,
- numbers of payment or credit cards,
- card validity dates,
- CVV2 codes of VISA credit cards (3 last digits on the right-hand side of the card holder signature strip).

1.3.4 Regularly update the system installed on your computer

Take interest in the updates of the system, which impact its security.

If you use Microsoft Windows, you should use the automatic Windows update option. Access to this option can be obtained in two ways:

- By selecting the Windows Update option in the Start menu of your Windows system
- By typing the following address into your browser http://windowsupdate.microsoft.com

There is also security information on the Microsoft Windows website:
http://www.microsoft.com/security/protect/default.asp

If you use another operating system, check the producer’s website, and if possible, join the mailing list for information about its updates.
1.3.5 Do not install software from sources which you do not trust

The simplest way to install hostile software in the system is to trick the computer owner to perform an installation of his own. One should be very circumspect about programmes downloaded from the Internet.

**Do not install software sent by e-mail.**

Never open files with the .exe extension whose origin is unknown. Often .exe programmes in the background install additional programmes extracting information from the computer (spyware) or giving full access to it via Internet.

1.3.6 Never use Millenet from publicly available computers

Never enter confidential data (Millenet, login, passwords) from a computer accessible to many persons, in particular in internet cafes and other public places. Data intercepting software can also be installed on them.

1.3.7 Take good care of the security of your passwords!

- Never reveal your passwords to anyone
- Passwords should be changed at least once a month (in Millenet you can set password change reminders from 7 to 60 days)
- Do not write down passwords or e-mail them
- If you think that someone might have already learnt your password – change it as soon as possible
- Passwords should differ from each other and from MilleKod and be difficult to guess.

1.3.8 Always select „Log Out” to finish your Millenet session

Always correctly close a Millenet session by clicking **Log out** from the horizontal menu.

1.4 Internet Certificates

The Certificate is to strengthen the level of Millenet security – without the Certificate access to account information is impossible and no operations can be carried out.

**Please note!** In the event of using more than one computer you need to install the Certificate on each computer.

To carry out operations in Millenet, the user should download and install an Internet certificate. Users may obtain Internet certificates from Millenet – as described in chapter: **How to Download an Internet Certificate?**

Millenet enables to download and install an Internet certificate through the **Administration – Download certificate** option. After downloading an Internet certificate, it must be authorised in accordance with the Client-defined Authorisation Rules.

If the Client needs mobility, he needs to install the Internet certificate on the laptop. Please note! An Internet certificate is valid for one year from the installation date.
## 1.5 Dictionary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement</td>
<td>Agreement for using Electronic Banking Channels concluded between the Bank and the Client.</td>
</tr>
</tbody>
</table>
| Client       | 1) Legal persons,  
2) Organisational units not possessed of legal personality, if they have legal capacity or ability to contract obligations,  
3) Natural persons running an income-earning business for their own account, including also persons running a farm.                          |
| MilleKod     | A sequence of signs (always 8-digits, if the Application specifies fewer digits, then they should be complemented by inserting the appropriate number of zeros at the beginning) in order to verify the Client in the system. |
| Login        | Identifier to be employed by the user when logging on to Millenet. The Client may specify any sequence from 4 to 20 signs (characters or digits).                                                             |
| Password     | A sequence of signs, consisting of 8 to 24 signs, is used for User authentication and in connection with MilleKod and User Login verifies that the user who is logging on to the system has been authorised by the client to use it. |
| The User     | The natural person who was given by the Client privileges to use the Millenet system.                                                                                                                      |
| Session      | Access to Client accounts kept by the Bank, which is established by giving MilleKod, User Login, and then their authentication with the use of a Password. Additionally, with the use of the Internet Certificate it is possible to reallocate funds accumulated on the bank account by means of Millenet. |
| Authorisation| Acceptance by a user having suitable privileges to order transactions.                                                                                                                                       |
| SMS P@ssword | One-time code texted to the mobile phone. It is used to approve operations in the Millenet for Companies Internet Banking System.                                                                           |

**Please note!** The system distinguishes big and small letters, but does not accept Polish characters.
1.6 How to Get Access to Millenet?

To get access to the Millenet Internet banking system contact your Relationship Manager or visit any Bank Branch and fill out the Application\(^1\) for Using Electronic Banking Channels.

Moreover, each new Client should provide:

- Personal data of all the users who will have access to the Millenet system (a xerox copy of an identity document of each of the users is additionally required),
- Scope of privileges of particular employees,
- Accounts to which they will have access,
- Authorisation rules depending on types and amounts of transactions which will apply to operation approvals (e.g. transactions of sending transfers or managing privileges in the system).

After having verified the completeness and correctness of the Client’s data each of the users will receive envelopes with passwords for logging in for all the users. The passwords are not active until the Client’s activation by the Bank. The number of the new MilleKod and possibility of access to Millenet shall be communicated to the client by the Bank.

Having received MilleKod you will be able to perform the first logging on to the system (activation). But access to information about accounts and transactions shall only be possible after downloading the certificate.

Please note! After logging on to the system every user should download the Internet certificate.

Information on the Certificate please find in the following subitems: How to Download an Internet Certificate? and Verification of the Internet Certificate

Should you have any questions or doubts please contact the Bank by calling 0 801 632 632 or + 48 22 598 40 31 or directly the Relationship Manager.

\(^1\) Hereinfrom called „Application“
2 Starting Your Millenet Session

2.1 First Logging on to Millenet

To use the Millenet service type [www.millenet.pl](http://www.millenet.pl) into the browser. Then on the logging screen type MilleKod (sent by the Bank by telephone) and click Companies.

The Client’s authentication window will appear (which is empty during the first logging, and during the later loggings will contain the Certificate downloaded by the User). Click OK, in order to continue loading the page.
Please note! If the window contains other Certificates select Cancel.

After loading the page you can see the MilleKod, which has been typed earlier.

- In the Login field enter the appropriate number from the „Application”; the Login is any sequence from 4 to 20 signs (characters or digits). The User’s Login must be compliant with the one given in the „Data of the Millenet User” Form
- In the Password field enter the User password (from an appropriate envelope).

After entering the data press Log on.

After the first logging the change of the User password will be enforced, whereby one should retype:

- Login compliant with the number from the „Application” or changed by the User to any sequence from 4 to 20 signs (characters or digits);
- Password (in accordance with the password from the envelope)
- New password (must be different than the one contained in the envelope – the new password may consist of numbers and characters, from 8 to 24 signs.

Then click Send to confirm the password.
Please note! The system does not accept Polish characters.

Please note! Three wrong entries of the Login or Password shall block the User’s access to Millenet. It can be unblocked only by the user having the privileges to do so granted in the system. If the User’s password originally created by the Bank is blocked, please report to the Millennium branch or to the Relationship Manager to obtain a New password/Passwords for logging.

After the first logging you can see the main window and the following message is displayed:

In order to gain access to information on accounts and carry out transactions through Millenet, each User must download and register the Internet Certificate. For this purpose click Continue.

Please note! In order to gain access to accounts through Millenet from other computers you must download and install the Internet certificate on each computer. For this purpose select „Continue”
2.2 Using the System

2.2.1 How to Download an Internet Certificate?

After clicking Continue or selecting from the left-hand side menu the option Administration - Download certificate you can see the screen: Generating certificate:

In the field Name of certificate enter any name (of your own) of the certificate (for better identification).

After clicking Continue the installation of the Internet certificate will start.

![Generate Certificates]

The next screen will bring information: "This website demands a new certificate on your behalf....".

![Potential Scripting Violation]

After clicking Yes the system will start to create and install the certificate and install it by showing appropriate information:

![Potential Scripting Violation]

Then press Yes.
The system will start generating certificate and show where to click **Add**

**Generate Certificates**

The Internet Certificate: 50-B0-FB-22-00-00-00-00-02-83
millenet.pl - CertificateName - 2009-08-05
valid until 05-08-2010, has been successfully loaded onto your Computer.
Click Add to perform certificate registration in the system.

Click **Yes** again and enter the SMS P@ssword received on your mobile and confirm **OK**.

**SMS password**

SMS with Password has been sent to your mobile. Please, read it and check to make sure that it’s details are consistent to data presented below:

Operation No. 1
from 2009-08-06
Adding certificate
Login: test
Serial no.: 50-B0-00-00-02-83
Expiry date: 2010-08-06

Enter received SMS Password to confirm data and click OK to execute operation

SMS password

* Required field

Generate new SMS password  Cancel  OK

A successful installation of the Internet certificate shall be confirmed by an appropriate message:

**Generate Certificates**

The Internet Certificate has been successfully registered in the system.
Please close the browser, reopen it and logon using your newly generated certificate.

Close your browser

Click **Close browser** to finish the process.
2.2.2 Verification of the Internet Certificate

After completing the process of downloading the certificate you can start working with Millenet. After opening the browser select address [www.millenet.pl](http://www.millenet.pl) and enter MilleKod and then select Companies. The certificates container will appear – this time it will contain the Certificate downloaded and installed by you:

![Client Authentication](image)

Having selected OK correctly log on to the system.

After the correct logging the system will recognise that during the previous session the certificate was downloaded. This will be confirmed by an appropriate message:

![Certificate download completed](image)

After clicking on Check certificate, the system will carry out an automatic control of certificate installation. If the verification is successful, the appropriate message will be displayed:

![Your certificate has been verified](image)

Press Start to use Millenet.
To check if the Internet certificate has been installed, select from the menu the function **Administration - Registered certificates**:

![Digital Certificates Management](image)

2.3 **Logging with the Use of the Internet Certificate**

Having performed the operations described in the previous chapters, the user may log on to the system with the use of the Internet certificate.

To do this open a new browser window, and type the system address: www.millenet.pl in the appropriate field or select it from the list „Favourites”, if it previously was added to it.

Then enter **MilleKod** and press **Companies**.

![milleNet Login](image)

In the process of opening the page the window: **Client’s authentication** will appear, but this time it will contain the installed Internet certificate (like in the window below):
Select the appropriate Internet certificate (if more than one were installed on the computer) and press OK. Then type the Login and current Password and click Log on.
2.4 Main Window – What does the User See after Logging on to the System?

After logging on to Millenet you can see the main window, which is also available after clicking the Start option in the horizontal menu.

The name of the Corporation appears as the name of the logged User. So in order to type the logged User’s data, make the appropriate changes.

The main page includes the following information:

- **Operations for authorisation entered by other users** – operations which can be accepted by the logged User – are not visible if the user employs the system for the first time.

- **Operations awaiting authorisation, entered by the user** – operations awaiting authorisation by other Users, – are not visible if the user employs Millenets for the first time,

- **Received messages from the user**.
Please note! Operations awaiting authorisation shall appear only, if the system is used by more than one user.

2.5 Actions after First Logging

Users who received envelopes with the P@ssword have full privileges in the system (with the automatically assigned A) profile and can use them only after selecting and registering the Internet certificate. One of the operations, which the user can carry out at any moment, is the modification of own personal data.

2.5.1 Changes of Screen Settings

Clicking Profile will open the page:

<table>
<thead>
<tr>
<th>Display options</th>
<th>Personal Information</th>
<th>Security settings</th>
<th>Password manager</th>
</tr>
</thead>
</table>

**Display options**

**New messages**

Lines per page: 9

**Transaction history screens**

Lines per page: 25

The parameters contained in this window allow to personalise the main page (available after pressing Start). The user has a choice of several settings relating to the number of message topics received from the Bank, which will be presented on the main page (from 1 to 4) and settings relating to the items of the history of transactions on the account – 25, 50 or 100.

2.5.2 Entering User’s Personal Data

After pressing Profile - Personal data the following page will open:
On this page personal data of the currently logged user are presented. By selecting the option **Edit** the user can make his own changes in the following parameters:

### Personal information

#### User Data
- Login
- Profile
- Can be an authorising user?

#### Personal data

<table>
<thead>
<tr>
<th>Personal data</th>
<th></th>
<th>Citizenship</th>
<th>Resident type</th>
<th>Father’s First Name</th>
<th>Mother’s Maiden Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Second name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date of birth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Place of birth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Identity Data
- PESEL
- NIP

#### Identity Documents

<table>
<thead>
<tr>
<th>Document #1</th>
<th>Document #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Type of ID</td>
<td>Name/Type of ID</td>
</tr>
<tr>
<td>Series/Number</td>
<td>Series/Number</td>
</tr>
<tr>
<td>Issue by</td>
<td>Issue by</td>
</tr>
<tr>
<td>Date of issue</td>
<td>Date of issue</td>
</tr>
<tr>
<td>Valid through</td>
<td>Valid through</td>
</tr>
</tbody>
</table>

#### Permanent Address
- Street
- House
- Apartment
- Postal code
- City/Town
- Country

#### Correspondence Address
- Street
- House
- Apartment
- Postal code
- City/Town
- Country

#### Contact Data
- Office email
- Mobile: +48
- Office Stationary Phone

---

Bankowość internetowa dla Przedsiębiorstw/ Instrukcja Użytkownika
Strona 27
## Personal Information

### User Data

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>asia</td>
</tr>
<tr>
<td>Profile</td>
<td></td>
</tr>
<tr>
<td>Can be an authorising user?</td>
<td>✔️</td>
</tr>
</tbody>
</table>

### Personal Data

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>M</td>
</tr>
<tr>
<td>First name</td>
<td>Jan</td>
</tr>
<tr>
<td>Second name</td>
<td></td>
</tr>
<tr>
<td>Last name</td>
<td>Kowalski</td>
</tr>
<tr>
<td>Date of birth</td>
<td>1975-01-01</td>
</tr>
<tr>
<td>Place of birth</td>
<td>Warszawa</td>
</tr>
<tr>
<td>Citizenship</td>
<td>Polish</td>
</tr>
<tr>
<td>Resident type</td>
<td>Resident in PL</td>
</tr>
<tr>
<td>Father's First Name</td>
<td></td>
</tr>
<tr>
<td>Mother's First Name</td>
<td></td>
</tr>
<tr>
<td>Mother's Maiden Name</td>
<td>Komak</td>
</tr>
</tbody>
</table>

### Identity Data

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PESEL</td>
<td>1111111111</td>
</tr>
<tr>
<td>NIP</td>
<td>1111111111</td>
</tr>
</tbody>
</table>

### Identity Documents

#### Document #1

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Type of ID</td>
<td>ID document</td>
</tr>
<tr>
<td>Series/Number</td>
<td>AAB6555</td>
</tr>
<tr>
<td>Issue by</td>
<td></td>
</tr>
<tr>
<td>Date of issue</td>
<td>2001-01-01</td>
</tr>
<tr>
<td>Valid through</td>
<td>2010-01-01</td>
</tr>
</tbody>
</table>

#### Document #2

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Type of ID</td>
<td>Choose</td>
</tr>
<tr>
<td>Series/Number</td>
<td></td>
</tr>
<tr>
<td>Issue by</td>
<td></td>
</tr>
<tr>
<td>Date of issue</td>
<td></td>
</tr>
<tr>
<td>Valid through</td>
<td></td>
</tr>
</tbody>
</table>

### Permanent Address

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Street</td>
<td>Aloha</td>
</tr>
<tr>
<td>House</td>
<td>1</td>
</tr>
<tr>
<td>Apartment</td>
<td>1</td>
</tr>
<tr>
<td>Postal code</td>
<td>11111</td>
</tr>
<tr>
<td>City/Town</td>
<td>Warszawa</td>
</tr>
<tr>
<td>Country</td>
<td>Poland</td>
</tr>
</tbody>
</table>

### Correspondence Address

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Street</td>
<td></td>
</tr>
<tr>
<td>House</td>
<td></td>
</tr>
<tr>
<td>Apartment</td>
<td></td>
</tr>
<tr>
<td>Postal code</td>
<td></td>
</tr>
<tr>
<td>City/Town</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>Choose</td>
</tr>
</tbody>
</table>

### Contact Data

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td>123123123</td>
</tr>
<tr>
<td>Country</td>
<td>Poland</td>
</tr>
<tr>
<td>Office Stationary Phone</td>
<td></td>
</tr>
</tbody>
</table>
• name and surname,
• type of profile,
• possibility of the user’s authorisation,
• nationality,
• resident status,
• date and place of birth,
• parent names,
• mother’s maiden name,
• PESEL
• NIP
• type and number of identity document,
• issuer, date of publishing and date of expiry of the identity document,
• registration address,
• address for correspondence (if different than the registration address)
• e-mail,
• landline,
• mobile phone (this is the number to which there SMS P@sswords will be sent),

2.5.3 Change of Security Settings

For security reasons the system has a parameter which will cause a timing-out of a session (logging out) in the event of a longer interruption in working with Millenet. This parameter can be user-defined.

After selecting Profile - Security settings the following page will open:

*Display options* | *Personal information* | *Security settings* | *Password manager*

**Security settings**

Your security settings: Minimum

Idle time: 15 mins

Password Reminder Frequency: 60 days

The page presents the currently defined time out values after which the system will automatically disconnect the session and the frequency with which it will remind about the possibility (but not necessity) of changing the password.

**Please note!** Inactivity is understood as lack of exchange of any data between the Bank and the user, therefore typing transfer data is treated as the user’s inactivity in the system. Thus, if the timeout value selected by you in the system is too short (e.g. 3 minutes), this may cause problems in your work in the system, namely frequent network disconnections. For example, after typing the transfer data and pressing Accept the system will return to the logging page and the typed data will be lost.

The user can select from three default settings: Minimum (respectively: 15, 60), Medium (7, 30), Maximum (3, 7) or own definition.

As the timeout parameter you can select any value in minutes between 1 and 15.

For the Password change reminder you can set any value between 7 and 60.
After the data entered in the Security settings have been updated log out and log on to the system once again.

### 2.5.4 Change of Password

This option allows the user to freely and at any time change the Password to the system.

After pressing: **Profile - Password settings** the following page will open:

![Password manager page](image)

To change a password type correctly the existing password, a new password of your choice, then retype the new password and save the change.

For the new password to be updated, log out and log on to the system once again.
2.6 How Can you Create a New User?

The Client (Firm) may at any moment decide to expand the earlier-defined structure of users.

In order to create a new user, click: Administration – New user.

On the displayed screen:
- Enter the new Login (any sequence from 4 to 20 characters),
- choose the password for the new user (sequence of characters and digits with the length from 8 to 24 signs, and then retype it (in the window below),
- decide if the user will have the authorisation possibility,
- assign to him an appropriate profile. There are three possible Profiles to be selected from: A, B or C. The granted Profile guarantees the possibility of carrying out particular transactions, in accordance with the Client-defined rules,
- enter detailed User’s personal data, as described in chapter: Entering User’s Personal Data

---

**User Management – New User**

**User Data**
- **Login**: [Input field]
- **Profile**: [Dropdown list] A, B, C
- **Can be an authorising user?**: [Checkbox]
- **Enter new password**: [Input field] (Password must have 8 to 24 alphanumeric characters)
- **Confirm new password**: [Input field]
- **Require password change**: [Checkbox]

**Personal data**
- **Gender**: [Dropdown list] Male, Female
- **First name**: [Input field]
- **Second name**: [Input field]
- **Last name**: [Input field]
- **Date of birth**: [Input field] (yyyy-mm-dd)
- **Place of birth**: [Input field]

**Identity Data**
- **PESEL**: [Input field]
- **NIP**: [Input field] (Digits only)

**Identity Documents**

<table>
<thead>
<tr>
<th>Document #1</th>
<th>Document #2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name/Type of ID</strong>: [Choose]</td>
<td><strong>Name/Type of ID</strong>: [Choose]</td>
</tr>
<tr>
<td><strong>Series/Number</strong>: [Input field]</td>
<td><strong>Series/Number</strong>: [Input field]</td>
</tr>
<tr>
<td><strong>Issue by</strong>: [Input field]</td>
<td><strong>Issue by</strong>: [Input field]</td>
</tr>
<tr>
<td><strong>Date of issue</strong>: [Input field] (yyyy-mm-dd)</td>
<td><strong>Date of issue</strong>: [Input field] (yyyy-mm-dd)</td>
</tr>
<tr>
<td><strong>Valid through</strong>: [Input field] (yyyy-mm-dd)</td>
<td><strong>Valid through</strong>: [Input field] (yyyy-mm-dd)</td>
</tr>
</tbody>
</table>
Please note! The user with Profile A may replace in operations the users with the remaining Profiles (i.e. B and C), while the user with Profile B can replace in operations users with Profile C.

Having entered the data click **Save**. The system will generate the user’s data for approval. After verification press **OK**.

Then enter the **SMS** password received on the mobile phone and click **OK** to carry out the operation. If you make a mistake, select **Cancel**.

**SMS password**

**SMS** with **Password** has been sent to your mobile. Please, read it and check to make sure that it’s details are consistent to data presented below:

**Operation No. 2**
from 2009-10-23
Create New User
with login:
and Profile:
Mobile number:

Enter received **SMS Password** to confirm data and click **OK** to execute operation

**SMS password**

* Required field

Having selected **OK** you will receive the message, where the option: **Download document** should be selected.

Print the document and press **Start**.
User Management

Operation executed successfully

In order to complete the procedure of user data update, it is essential to deliver to the Bank the authorised printout of User Data Form together with a copy of the identification document(s).

**If you are a Bank Millennium Business Customer:**
Please deliver the documents to a Bank Millennium branch of your choice.

**If you are a Bank Millennium Corporate Customer:**
Please send the User Data Form to the address given in the Millenet mail message you received, or hand it directly to your Relationship Manager.

The printed out form with updated data and copy of the user’s identity card should be supplied by the client to the Bank’s Relationship Manager or any branch of the Bank.

Please note! The user despite the entered personal data has no privileges in the Millenet system.

The next step in creating the new user is to assign to him the privileges to perform particular operations in the system.

Reselect the option: Administration - User details. Select the newly created Login and move to the tab Operations Allowed. Click the Edit option to grant privileges to the User. The detailed description of the privileges is presented in subitem: Granting User Privileges to Perform Individual Operations.
Having accepted Save, and then Start do as in the case of introducing personal data. Print the document with updated privileges of the new user, and then confirm the operation with the SMS Password. The detailed description of granted privileges to perform operations are presented in subitem: Granting User Privileges to Perform Individual Operations.

Please note! The user despite the entering of personal data and granting privileges does not have access to particular accounts.

The next step in creating a new user is to give him access to particular accounts. Again, please select the option Administration - User details. Then select the newly - created Login and move to Accessible accounts.

Having selected Edit you can select (by ticking the selection window) the accounts, which we want to be accessible to the new User.
After clicking Save, and then Start, do as in previous cases. Then select documents with accessible accounts for the new user. Use the SMS password to confirm the operation and click OK.

Granting access privileges to particular accounts is described in detail in subitem: Granting User Access to Particular Accounts

Please note! The full set of documents (Personal data with a copy of documents, list of privileges to Millenet, list of access to particular accounts), should be supplied by the Client to the Relationship Manager or any Bank branch.

Please note! A new user may perform operations in the system only after downloading and installing the Internet certificate, as explained in subitem: How to Download an Internet Certificate?

### 2.7 Modification of User Privileges

No matter what profile is selected for a given user, you can always additionally modify the scope of operations available for each User irrespective of the Profiles granted to them.

Click Administration – List of users to trigger a page with additional elements of the menu:

- **User Data** – under this option you can make changes in the User Profile and assign a new password to other users in the case their access is blocked or password forgotten,

- **Operations allowed** – here you can modify the set of operations to which a given user will have access,

- **Accessible accounts** – here you can define the set of accounts on which a given user will be perform operations and views.

#### 2.7.1 Granting User Privileges to Perform Individual Operations

In order to modify User privileges to exercise particular functions, click Administration - User details. By default, the system will display grouped privileges of access to the operations of the currently logged user.
Then select the **Login** of the User who will be changed his access privileges. We have thus a possibility of overviewing the groups of operations to which the selected user has access.

Operations are divided into groups which correspond to the rules of performing particular operations:

From here you can grant or withdraw privileges to perform particular operations:

- **Assets and liabilities** – access to information on total balances in particular groups: current accounts, term deposits, cards, loans,
- **Current accounts** – full view (allows to view detailed information on transactions on accounts),
- **Upcoming payments** – allows to view the list of defined payments for a selected period in future – the default is 1 month / 2, 3 and 12; standing order payments, transfers with future execution date, repayments of loan instalments, etc.,
- **Transfers** – after opening this group of operations you can grant access to the following transfers:
  a) transfer between Company accounts with future execution date,
  b) transfer between Company accounts,
  c) domestic transfer,
  d) domestic transfer with future execution date,
  e) foreign transfer,
  f) pending transfers – list,
  g) postal transfer,
h) postal transfer – editing,
i) pending transfer – removal,
j) SORBNET transfer on request,
k) tax transfer,
l) pending transfer – modification,
m) 3 in 1 ZUS transfer
n) pending foreign transfers – list
o) rejected foreign transfers list.

- **Standing orders:**
  a) Standing order – adding,
  b) Standing order – list,
  c) Standing order – removal,
  d) Standing order – editing.

- **Term deposits:**
  a) term deposit – setting up,
  b) term deposit – detailed information,
  c) term deposit – list,
  d) term deposit – cancellation.

- **Cards:**
  a) card activation,
  b) card – detailed information,
  c) list of inactive cards,
  d) list of cards.

- **Loans:**
  a) guarantees and loans – list,
  b) investment loan – detailed information,
  c) investment loans – list,
  d) investment loan – schedule,
  e) renewable loan – detailed information,
  f) renewable loans – list.

- **Authorisations:**
  a) authorisation (signing an operation),
  b) history of authorisations of Company transactions,
  c) history of authorising own transactions,
  d) authorisation – cancellation (possibility of withdrawing a prepared operation requiring additional signatures. Such authorisation can be withdrawn only by the person entering the operation),
  e) authorisation – detailed information,
  f) authorisation – list,
  g) send (possibility of sending orders for execution),
  h) rule of transaction – saving (possibility of making changes in rules of transaction; modification of amounts and combinations of signatures),
  i) list of accessible accounts – (privilege to modify the list of accessible accounts for the users),
  j) list of operations allowed – (privilege to modify the list of operations allowed for the users),
  k) rule – list of all,
  l) operational rules – list,
  m) operational rule – modification (possibility of making changes in operational rules).

- **Setting up of users:**
  a) Users – new (adding a new user),
b) Users – information,
c) Users – list,
d) Users – removal,
e) Users – saving (saving of changes),
f) Emergency blockade of orders authorisation
g) Passwords recovery

- **Other services:**
  a) exchange rates,
b) ordering a statement duplicate,
c) ordering a transaction confirmation.

- **Internet certificates:**
  a) Adding an Internet certificate (possibility of reporting an Internet certificate for registration with the use of the **Add** option),
b) list of Internet certificates,
c) removal of an Internet certificate,
d) downloading an Internet certificate.
e) order a Certificate Download Password

- **Recipients:**
  a) recipient – adding,
b) recipient – removal,
c) recipients – removal (removal of the whole list)
d) recipient – editing,
e) adding a file with recipients.

- **Operations log:**
  a) log of all company operations.

- **Collective transfers:**
  a) collective transfer – removal (removal of the whole batch with transfers),
b) collective transfer – processing (sending a batch to be executed),
c) collective transfer – detailed information,
d) report from a collective transfer
e) list of collective transfers – list of previously registered batches,
f) collective transfer – adding (adding a batch with transfers),

- **Statements/Reports**
  a) AIPP reports – viewing daily reports of the automatic identification of incoming payments,
b) Online statements – define/edit – defining and changing the existing on-line statement definitions
c) Online statements – List – list of predefined online statements for downloading.

To start modification select **Edit**, and then add or remove all the Operations allowed, using default buttons or individually for each option.

Pressing **Save** will display the screen confirming the set definition. Then press **OK** to confirm and generate the **SMS P@ssword**. After entering the code and reconfirmation, the changes will be saved.

The next step is to download the document and supply it to the Relationship Manager or any Bank Branch.
2.7.2 Granting User Access to Particular Accounts

To edit the possibility of accessing particular accounts, select the option Administration - User details, then select Login of the User whose access to accounts will be modified and click the Accessible accounts tab.

In order to change the group of Accessible accounts, select the Edit.

Then select the accounts (by clicking the selection window) which should be available for the User.

Press Save, which will move you the screen presenting the given set of accounts available for a given User.
Next, press **Save** to save the changes.

**Please note!** If a new account is opened at the Bank, the User with administrative privileges should in the option **Administration – User details – Accessible accounts** grant administrative privileges to the Users who should have access to the account in question.

When making all the modifications of the User privileges enter the **Password SMS** received on the mobile and click **OK** to confirm.

**2.8 What do you Use Authorisations for and how do you Create Them?**

Authorisations are a Millenet functionality built especially for Companies in order to enable the mirroring of the privileges used in Companies to dispose of funds.

By defining a multiperson approval of operations you gain full internal control over executed operations, in particular financial operations going beyond your Company’s assets. In defining users with appropriate Profiles (A, B or C) and specifying how many users must authorise an operation, you introduce a multistage acceptance process which must be completed for the operation to be carried out.
In order to define in what combinations particular operations can be carried out, define these combinations along with the amount ranges in the option **Administration - Authorisation rules**:

### Amounts Authorizations Management

**Rules applied in currency: PLN**

#### Transfers outside Company’s assets

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>up to 10.00</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>up to 12.00</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>up to 30.00</td>
<td>AAA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 3 in 1 ZUS Transfer

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>up to 2.00</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>up to 15,000.00</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>up to 0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Transfers within Company’s assets

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>up to 1.00</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>up to 5.00</td>
<td>AB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>up to 1,000,000.00</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Term Deposits

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>up to 2,000.00</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>up to 15,000.00</td>
<td>CB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>up to 20,000.00</td>
<td>ABC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Millenet has the following groups of operations for which you can define signature combination rules:

- **Transfers outside Company assets** – combinations defined in this rule with the use of amount ranges will cover operations causing the debiting of funds from the Company’s accounts at Bank Millennium in favour of third parties. This rule also pertains to standing orders and folders with transfers (no matter if they are executed to accounts at the Bank or to other accounts).
- **ZUS 3 in 1 Transfer** - combinations defined in this rule with the use of amount ranges will cover operations causing the debiting of funds from the Company’s accounts at Bank Millennium to the Social Insurance Authority.
- **Transfers within Company assets** – combinations defined in this rule with the use of amount ranges will cover operations causing the transfer of funds between Company accounts at Bank Millennium.
- **Term deposits**,
• **Recipients** – set of combinations in accordance with which you can add, modify or remove Recipients.
• **Authorisation rules** – set of combinations according to which you can change rules.
• **Internet certificates** – set of combinations according to which the registration of Internet certificates is performed.
• **Users** – set of combinations according to which you can modify User privileges.

The below-presented rule for **Transfers outside company assets** should be understood as follows:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 1,000,00</td>
<td>CCC</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>2 to 10,000,00</td>
<td>AA</td>
<td>BBB</td>
<td></td>
</tr>
<tr>
<td>3 to 1,000,000,00</td>
<td>AAA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If the Client wants to perform a transfer for the amount of 500,00 PLN, then this amount is contained in the range defined in line 1 and such transfer will be carried out, if it is authorised (signed) by three users with profile C or by one User with profile A.

**The system will carry the transaction, if one of the acceptable combinations is satisfied.**

### 2.9 Specimen Configuration – Users and Authorisation Rules

Millenet is activated for different numbers of users defined by the Client. Its construction is so flexible that it enables the Clients to adjust the structure of system users and rules of carrying out particular operations depending on the needs at a given moment.

The subitems below include specimen illustrations of selected configurations which the Client could use for granting Profiles and Authorisation Rules to the Users.

#### 2.9.1 Initial Configuration

##### 2.9.1.1 Initial Configuration with two Users

When Millenet is activated with two Users, the Client will receive **MilleKod** from the Bank, two **Login** numbers (defined by the User) and two **safe envelopes** containing the Password enabling the first logging on to the system for created Users.

The originally created Users have an automatically assigned Profile A and access to all operations in the system. All the rules defined in the system will contain only one combination defined as presented in the table:

**Transfers outside Company assets:**

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000,00</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0,00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0,00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**3 in 1 ZUS Transfer:**

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000,00</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0,00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0,00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Transfers within Company assets:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000.00</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Term deposits:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000.00</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Authorisation rules:

<table>
<thead>
<tr>
<th>Type of operation</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorisation rules</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificates</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recipients</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This means that in order to carry out each operation by one of the Users, it must be approved by the other User.

2.9.2 Small Business

2.9.2.1 Owner

Below please find the configuration for a sole trader company.

If there are two users in the initial configuration of the system, for one user to be able to use the system on his/her own, the Authorisation Rules must be changed from „AA“ to „A“.

Transfers Outside Company Assets:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 100,000.00</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3 in 1 ZUS Transfer:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 100,000.00</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Transfers within the Company assets:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 100,000.00</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Term deposits:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 100,000,00</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0,00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 0,00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Authorisation rules:

<table>
<thead>
<tr>
<th>Type of operation</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorisation Rules</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificates</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recipients</td>
<td>A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If the above mentioned combinations are implemented in the system only one User will have full privileges in Millenet. The next steps of introducing the above-mentioned combinations are described in chapter:

**2.9.2.2 Owner + Assistant**

Below please find a possible configuration for a small company – one owner cooperating with an assistant. The service will be activated for two initial users with appropriate rules („AA” for all types of operations). The owner performs the role of two Users created by the Bank – he downloads and activates Internet certificates.

Then, the Owner by using both Profiles changes (and authorises) the Authorisation rules from „AA” to the below-proposed one, finally changing the Profile of one of the Users for the Assistant from A to C.

Transfers outside Company Assets:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000,00</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100,000,00</td>
<td>CA</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 0,00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3 in 1 ZUS Transfer:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000,00</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100,000,00</td>
<td>CA</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 0,00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Transfers within Company assets:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000,00</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100,000,00</td>
<td>CA</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 0,00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Term deposits:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000,00</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100,000,00</td>
<td>CA</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 0,00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Authorisation rules:

<table>
<thead>
<tr>
<th>Type of operation</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorisation rules</td>
<td>A CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificates</td>
<td>A CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>A CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recipients</td>
<td>A CA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In accordance with the presented rules User C shall be able to carry out on his own operations up to 5,000.00 PLN for an individual transaction.

For transactions with higher amounts and in operations not connected with amounts User C shall not carry out operations on his own. But User A will always be able to carry out any operation on his own.

2.9.2.3 Two Co-owners + Assistant

Below we present a possible configuration for a small corporation – two co-owners cooperating with an Assistant.

This service shall be activated for two initial Users (for Co-owners), with appropriate rules („AA“ for all types of operations). The Users will download and activate Internet certificates.

Then, one of the Users A will create a new User, e.g. with Profile C, by assigning to him the right of access all the operations. Such operation will need to be approved by the second User A.

The User with Profile C (Assistant) must download the Internet certificate, and the Internet certificate will be registered by Users A by placing two signatures.

Then, User C will enter operations in the System, while the User with Profile A will approve them for execution. To this end you can modify the rules to the following form:

Transfers outside Company assets:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000.00</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100,000.00</td>
<td>CA</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 500,000.00</td>
<td>CAA</td>
<td>A</td>
<td>AA</td>
</tr>
</tbody>
</table>

3 in 1 ZUS Transfer:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000.00</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100,000.00</td>
<td>CA</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 0,00</td>
<td>CAA</td>
<td>A</td>
<td>AA</td>
</tr>
</tbody>
</table>

Transfers within Company assets:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000.00</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100,000.00</td>
<td>CA</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 500,000.00</td>
<td>CAA</td>
<td>AA</td>
<td></td>
</tr>
</tbody>
</table>

Term deposits:

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5,000.00</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100,000.00</td>
<td>CA</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 500,000.00</td>
<td>CAA</td>
<td>AA</td>
<td></td>
</tr>
</tbody>
</table>

Authorisation rules:
<table>
<thead>
<tr>
<th>Type of operation</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorisation rules</td>
<td>AA</td>
<td>CA</td>
<td></td>
</tr>
<tr>
<td>Certificates</td>
<td>AA</td>
<td>CA</td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>AA</td>
<td>CA</td>
<td></td>
</tr>
<tr>
<td>Recipients</td>
<td>AA</td>
<td>CA</td>
<td></td>
</tr>
</tbody>
</table>

Such definition of the rules means that a Profile C user will be able to carry out transactions on his own up to the amount of 5,000,00 PLN.

Transactions up the amount of 100,000,00 PLN can be performed by each of the co-owners on their own.

Transactions above the amount of 100,000,00 PLN to 500,000,00 PLN can be carried out with the joint consent of the two co-owners.

But operations connected with the amounts can be carried out by two Users with Profile A or combinations of the Users C and A.

### 2.9.3 Bigger Structure

The below-described structure is an example of the definition of the division of functions in a bigger company, where different people are responsible for selected operations.

Hence, after the activating of the service originally for 2 Users, you can define additional Users like in the example:

- **User with Profile C** – with privileges (operations allowed) of access to:
  - a) Handling of collective transfers,
  - b) Transaction authorisation,
  - c) Handling of Internet certificates,

Such user will be able to add (send to the Bank, but not send for execution) folders with transfers.

- the **User with Profile C** – with privileges (Operations Allowed) of access to:
  - a) Transfers
  - b) Recipients,
  - c) Cards,
  - d) Access to detailed information on accounts,
  - e) Transaction authorisation,
  - f) Handling of Internet certificates

Such user will be able to make domestic transfer orders (in PLN to company accounts at Bank Millennium, to other banks, to ZUS (Social Insurance Authority), to the Tax Office and foreign transfers or in currency transactions).

It is possible to separate the access of Users to types of transfers, e.g.: only transfers between company accounts at Bank Millennium, only domestic transfers, only ZUS, only Tax Office and only currency transactions or other configurations.

- **User with Profile C** - with privileges (Operations Allowed) of access to:
  - a) Term deposits,
  - b) Standing orders,
  - c) Cards,
  - d) Access to detailed information on accounts,
  - e) Transaction authorisation,
  - f) Handling of Internet certificates

- the **User (or 2 Users; here replaceability)** with Profile B – with privileges (Operations Allowed) of access to:
  - a) Transfers
  - b) Standing orders,
c) Cards,
d) Term deposits,
e) Recipients,
f) Transaction authorisation,
g) Handling of Internet certificates.

Such user will be able to authorise (accept transfers for lower amounts). In addition to this you can make available transfer functions as a whole and collective transfers.

- In such system configuration there are 6 users in the system:
  a) Two with profile A with full access privileges,
  b) Two with Profile B with dedicated access privileges,
  c) Three with Profile C with dedicated access privileges
  d) Definition of the rules for such number of Users may look as follows:

**Transfers Outside Company Assets:**

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 2.000,00</td>
<td>CB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100.000,00</td>
<td>BA</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 500.000,00</td>
<td>BBA</td>
<td>AA</td>
<td></td>
</tr>
</tbody>
</table>

**3 in 1 ZUS Transfer:**

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 2.000,00</td>
<td>CB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100.000,00</td>
<td>BA</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 500.000,00</td>
<td>BBA</td>
<td>AA</td>
<td></td>
</tr>
</tbody>
</table>

**Transfers within Company assets:**

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5.000,00</td>
<td>CB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100.000,00</td>
<td>BB</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 500.000,00</td>
<td>BBA</td>
<td>AA</td>
<td></td>
</tr>
</tbody>
</table>

**Term Deposits:**

<table>
<thead>
<tr>
<th>Amount</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>to 5.000,00</td>
<td>CB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 100.000,00</td>
<td>BB</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>to 500.000,00</td>
<td>BBA</td>
<td>AA</td>
<td></td>
</tr>
</tbody>
</table>

**Authorisation Rules:**

<table>
<thead>
<tr>
<th>Type of operation</th>
<th>Combination 1</th>
<th>Combination 2</th>
<th>Combination 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorisation Rules</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificates</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>AA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recipients</td>
<td>CB</td>
<td>B</td>
<td></td>
</tr>
</tbody>
</table>
Such definition of the rules means that a user with Profile C will only be able to enter transactions, but will never be able to carry them out on his own. The carrying out of each transaction up to the amount of PLN 5000,00 requires the consent (authorisation) of a User with Profile B, because the latter has the privileges to authorise (express consent). Additionally the scope of privileges for a given User will decide which area of the entered transactions and/or operations is the responsibility of a given user.

Transactions up to the amount of PLN 100 000 will be executable by at least two Users – in the case of delegating transactions to the Users lower in the hierarchy. At the same time the User with the highest empowerment in the hierarchy (Management Board) could carry out such transactions on their own.

Transactions above the amount of 100.000,00 PLN to 500.000,00 PLN shall be executable with the joint consent of two Users with Profile A of the Co-owners.

Operations of adding Recipients to the list will enterable by an appropriate User with Profile C or on their own by the User with Profile B.

On the other hand operations not connected with amounts and important in terms of security will always be carried out by Users with Profile A.

Please read User Instructions part II

Should you have any questions or doubts please contact the Bank by calling 0 801 632 632 or +48 22 598 40 31, of directly the Relationship Manager.