Aareal
YOUR COMPETITIVE ADVANTAGE.

Aareal Portal

Administrator Manual

Imprint

Documentation for the Aareal Portal, Release 7.8.4 of 17 January 2023

Aareal Bank AG
Banking & Digital Solutions division
Paulinenstrasse 15
65189 Wiesbaden

Table of Contents

1. Introduction

Welcome to the Administrator Manual for the Aareal Portal!

The Aareal Portal will help you and your employees handle your financial affairs regardless of whether you work in a small dynamic company with only a few employees or you want to assign complex workflows to a large number of employees for approving and checking payments.

For this purpose, the Aareal Portal can be customised in many different ways to suit your needs. For example, you can assign employees the specific rights they need for viewing information or executing payments.

This Administrator Manual will help you to understand and utilise the potential offered by the Aareal Portal and supplements the User Manual for the Aareal Portal, in which all functions required by users in their daily work are explained. If you wish to first familiarise yourself with how the Aareal Portal is utilised and what functions it offers, please start by reading chapters 4 and 5 of the User Manual.

The following pages set out all the information you need as an administrator to configure the Aareal Portal for your company.

Chapter 3 initially describes quick solutions for frequent situations occurring on a daily basis. This will provide you with quick answers so that you don't have to delve more deeply into the Manual.

Chapter 4 will offer you an overview of the individual steps that are necessary to set up users, the imageTAN reader and EBICS authorisations. It provides a common thread through the configuration of the Aareal Portal. Start with this chapter if you would like to learn how to configure the Aareal Portal and set up an initial configuration.

The other chapters describe individual aspects of administration:

- Chapter 5 provides all information on setting up and managing users.
- Chapter 6 shows you how to define access rights efficiently and assign them to users.
- Chapter 7 explains how to use imageTAN readers.
- Chapter 8 tells you how to link users with EBICS participants and thereby grant them corresponding rights to the defined accounts.
- Read about automatic and regular retrievals in Chapter 9.
- Finally, Chapter 10 will show you how to use activity logs to see swiftly and simply what users have performed what activities on the Aareal Portal.

We hope you enjoy using the Aareal Portal.

Conventions

To make this manual easier to follow, the formatting described below will be used throughout:

! ***Tip/note**: Practical tips and important notes are clearly set off with an exclamation mark and italic text.*

Operable **BUTTONS** on the Aareal Portal are written in small capital letters with a blue font.

Names of input fields as well as selection options are marked in **bold**.

2. Requirements

In order to use the Aareal Portal as an administrator, you require an active user with administration rights for your client logon. You will receive the initial logon data from Aareal Bank. Please set up this user in accordance with the instructions in chapters 2 and 3 of the User Manual.

If administrator rights have been assigned to your user ID, you can see this from the fact that, among other things, you can access the menu entry **USER** with various functions for user management in the **MANAGEMENT** module after you successfully log onto the Aareal Portal.

3. Quick start: How to ...

TEMPORARILY LOCK A USER.

Enter the MANAGEMENT module and select USER from the menu. Find the user you are looking for and then click on [+] at the end of the line. As soon as you click on LOCK, the user will be locked with immediate effect.

Further information can be found in chapter 5.2 on page 22.

UNLOCK A PREVIOUSLY LOCKED USER.

To unlock a previously locked user, you must request a new logon for that user and have him or her go through the initial logon process again.

Enter the MANAGEMENT module and select USER from the menu. Find the user you are looking for and then click on [+] at the end of the line. Click on REQUEST LOGON DATA, save the document that you are prompted to download and send it to the user.

The user can now log on again with this letter. The imageTAN reader remains activated so that no further action is required here. The EBICS keys stored in the key medium also remain active.

If, on the other hand, the user has locked himself or herself out, all the EBICS keys are also deleted for security reasons. Please remind the user to re-initialise the EBICS logons in this case.

Further information can be found in chapter 5.4 and in chapter 6.2.3 of the User Manual.

RESET THE PASSWORD.

To assign a new password to a user, you must request a new logon for that user and have him or her go through the initial logon process again.

Enter the MANAGEMENT module and select USER from the menu. Find the user you are looking for and then click on [+] at the end of the line. Click on REQUEST LOGON DATA, save the document that you are prompted to download and send it to the user.

The user can now log on again with this letter. The imageTAN reader remains activated so that no further action is required here. The EBICS keys stored in the key medium also remain active.

Further information can be found in chapter 5.4.

RESET THE ADMINISTRATOR PASSWORD.

If you have lost or forgotten the password for your client logon with administrator rights, please contact your client relationship manager at Aareal Bank, who will arrange for you to receive new logon data. In this case, your key will remain active so that you can continue to use it.

RESET THE DEVICE PIN.

If a user has forgotten the PIN that he or she has selected for the imageTAN reader, he or she can reset it himself or herself. To do this, he or she logs onto the Portal with his or her client ID, user ID and password and clicks on "PIN forgotten or locked?" on the login screen. The link is shown in Figure 18.

If you as the administrator want to reset the PIN for the user or if the user has forgotten his or her logon data, go to the **MANAGEMENT** module and enter the **IMAGETAN READER MANAGEMENT** menu. You can now revoke the licence for the imageTAN reader in question by clicking on **RESET KEY**.

In both cases, the key must be re-activated and, if necessary, a new EBICS key generated.

Further information can be found in chapter 7.3.1.

UNLOCK A USER WHOSE KEY IS SET TO "WAITING FOR APPROVAL" ON THE USER MANAGEMENT PAGE.

"Waiting for approval" is displayed for users in cases in which you have set the key to be subject to compulsory approval, meaning that it must be unlocked manually.

The user has activated his or her imageTAN reader and received a letter for downloading that includes the approval code. As soon as you have received this letter from the user, proceed to the user management page in the **MANAGEMENT** module by selecting **USER** from the menu. Now select the user in question and then click on **[+]** at the end of the line. Now click on **EDIT** and switch to the **KEY** tab.
You can then enter the approval code here: If the unlocking key is correct, this is shown by a green tick. **ACCEPT** and **SAVE** your settings.

Please note that administrator logons must be activated by Aareal Bank.

Further information and what to do if you lose the letter can be found in chapter 5.5.

REACT WHEN A USER HAS LOST HIS OR HER IMAGETAN READER.

If there is no doubt that the key has been lost, the first step should be to lock the device. This can be done either by the user or by you as the administrator on behalf of the user.

To lock the imageTAN reader, the user logs onto the Aareal Portal with his or her client ID, user ID and password and clicks on "Lock imageTAN reader" on the login page. The link is shown in Figure 18.

As the administrator you can also deactivate the user's imageTAN reader. In both cases, all EBICS keys are deleted when the imageTAN reader is locked. The advantage for you as the administrator locking the reader is that the user does not require any new logon data. In the MANAGEMENT module, go to the USER menu, select the user in question and EDIT his or her data. Now go to the Key tab and click on the button with the small counter-clockwise arrow.

Further information can be found in chapter 7.3.3.

IDENTIFY THE OWNER OF AN IMAGETAN READER.

Open the **Settings** menu of the imageTAN reader by switching off the device and holding down the on/off button at the top edge of the device for at least three seconds. Then select "Activation" to display the licence.

On the Aareal Portal go to the Management module, select the menu item IMAGETAN READER MANAGEMENT and enter the licence number of the device in the corresponding field.

The user ID with which the imageTAN reader is linked will now be displayed. If no user ID can be found, this means that the licence has already been revoked.

Further information can be found in chapter 7.3.4.

DEFINE LANGUAGE SETTINGS FOR AUTOMATICALLY GENERATED MESSAGES.

To alter the language settings for automatically generated messages for all users, go to the MANAGEMENT module and select USER. Now change the language using the "Language" selection box.

Further information can be found in Table 1 in chapter 5.

4. Setting up the Aareal Portal

The following chapter provides an overview of the administrative activities that are available on the Aareal Portal. Read through this chapter particularly carefully if you are not yet familiar with the administration of the Aareal Portal and initially want to gain an overall understanding.

Start with the administration of the Aareal Portal by setting up user IDs for your users and providing them with the imageTAN readers they need to log on with.
Read the chapters 5.1 and 5.4 further down in the manual for more information on these steps. We recommend reading all of chapter 5 to gain a deeper understanding of user administration.

As soon as he or she has completed these steps, the user can log onto the Aareal Portal, view all the data and pages on the Aareal Portal which he or she is authorised to access in accordance with the modules and roles assigned to him or her or any account restrictions that may have been defined. In particular, he or she may view payment data and account transactions that have been stored on the Aareal Portal, e.g. because they have already been retrieved from the bank server by another Portal user. Accordingly, a user can also view such data even in the absence of any signing powers, provided that no account restrictions have been defined for him or her.

If in addition to this the user is to be permitted to independently retrieve transaction data or send payment orders to banks or approve them, he or she requires the corresponding authorisation for this bank. This is done in the form of EBICS participant IDs that are assigned to individual users. The EBICS participant data is available from the bank advisor of the bank for which you require authorisation for the user.
Chapter 5.2 of the User Manual provides an overview of EBICS authorisations.

If you want to manage accounts held with other banks on the Aareal Portal in addition to your accounts with Aareal Bank, you must set up a bank parameter for the bank in question. The bank parameter describes the method for connecting to the core banking system of the external bank, thus providing the basis for secure communications between the Aareal Portal and your bank.
The bank parameter for your accounts with Aareal Bank has already been set up for you.

- Check whether your client logon has been activated for the inclusion of external banks. Table 1 in chapter 5 will help you with this.
  If your logon has not been activated and you would like it to be, contact your client advisor at Aareal Bank.
- Create a bank parameter for every bank which you would like to access from the Aareal Portal. This function is described in detail in chapter 6.2.1 of the User Manual.

Every user who, as described above, wishes to retrieve transaction data from the bank server or approve payment orders requires an EBICS participant ID, which he or she must initialise using his or her imageTAN reader to generate the keys required for communications.

- Assign each user who is to receive EBICS authorisation an EBICS participant ID. Chapter 8 describes the individual steps for doing this. Alternatively, the Portal user can do this himself or herself for his or her own user logon.
- As a last step, each user must initialise his or her EBICS participant ID. This is described in chapter 6.2.3 of the User Manual.

Your users are now set up and can work with the Aareal Portal.

So far, you have learned that there are various parts which play a specific role in the administration of the Aareal Portal. Let's reiterate this here:

- An employee logs on to the Aareal Portal with a user logon. The user can view data that has already been retrieved on the basis of his or her authorisation but cannot yet communicate with a bank server. The user requires an imageTAN reader to log onto the Aareal Portal.
  Everything you need to know about user logons can be found in chapter 5.

- The imageTAN reader is required by every user to log on securely to the Aareal Portal. In addition, it is used as a key medium for communications with the bank server, e.g. to approve payments or to retrieve transaction data.
  Chapter 7 explains the imageTAN reader in greater detail.

- The parts of the Aareal Portal that a user can access is determined by means of definable roles and by selecting the modules that are assigned to the individual user. More details can be found in chapter 6.

- If you want to manage accounts held with other banks on the Aareal Portal in addition to your accounts with Aareal Bank, you must set up a bank parameter for each bank. This forms the basis for communications with the bank server via EBICS. Chapter 6.2.1 of the User Manual will tell you how to set up bank parameters.

- Finally, each user wishing to send orders to banks via EBICS needs an EBICS participant ID, which must first be initialised.
  Chapter 8 describes in detail the process for assigning EBICS participant IDs to users. Chapter 6.2.3 of the User Manual describes the procedure for initialising EBICS participant IDs.

5. Setting up users

One of your most important tasks as an administrator is deciding which employees are to be able to log onto the Aareal Portal and which actions they are to be permitted to perform.

This chapter describes how to add new users to the Aareal Portal, define their rights, temporarily lock them or permanently delete them. It also explains how to restore a user's access to the Aareal Portal if that user has forgotten his or her password or lost his or her imageTAN reader.

There are three different logon types for the Aareal Portal:

- A *user* is a person who is able to log onto the Aareal Portal with his or her own logon data.
- An *administrator* is a user with additional rights for the administration of the Aareal Portal. The administrator can create new user logons and lock them or assign new logon data. He or she can grant user rights or define restrictions. In addition, the administrator can track activities on the Aareal Portal via the activity log and trace them back to individual users.
- An *Aareal Bank administrator* manages your client logon and is available to support you with certain activities. He or she can for example grant administrator rights to further users or change the name of your company. Some activities must necessarily be performed or confirmed by this administrator.

To create users or edit existing ones, open the **MANAGEMENT** module in the top menu line and select **USER**. The screen for managing users is displayed in Figure 1.

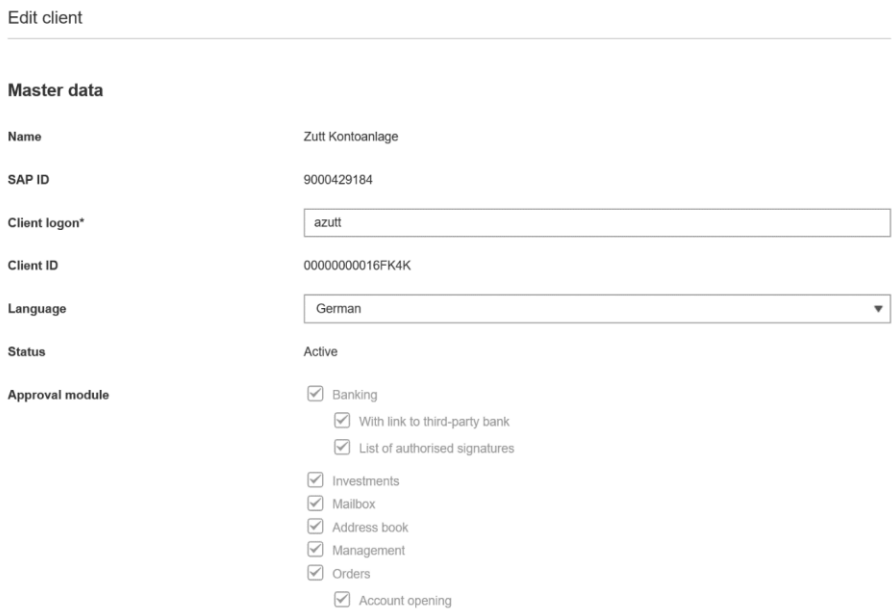

Figure 1: Displaying master data on the user management page

The page is divided into two parts. In the top part you will see the **Master data**, i.e. the information related to your client logon at Aareal Bank. This part contains the following details:

Name	The name of your company. This is assigned by Aareal Bank on the basis of the information that you provide when your client logon is created. Please contact your client advisor if any changes are required.
SAP ID	The 10-digit SAP ID together with your client ID links your client logon with Aareal Bank's core banking system.
Client logon	The client logon is freely selected by you and used to uniquely identify you on the Aareal Portal. You require your client logon to log onto the Aareal Portal, for example. You can modify your client logon anytime. Please remember to inform all users of the new client logon as otherwise they will not be able to access the Aareal Portal. The change becomes effective immediately upon being saved. When you select a new client logon, you can use numbers and all letters customarily used in the German-speaking region plus the following special characters: _ @ ! $ % & / ( ) = ? - | > < The client logon can have up to 15 characters and must not already be used by another client on the Aareal Portal. Click on **SAVE** at the bottom of the page to store your data.
Client ID	The client ID together with your SAP ID links your client logon with Aareal Bank's core banking system.
Language	The language setting selected here applies to the language of automatically generated notifications for all of a client's users. This includes messages in the mailbox, the other logs and the activity log and is independent of the specific user language settings for the user interface (see User Manual).
Status	This shows the current status of your client logon: active or inactive. If the client logon is deactivated, all users are automatically locked. For this reason, you will never see the status "inactive" for you as the client administrator. After your logon is re-activated by your Aareal client advisor, remember to unlock all locked users by requesting new logon data for each of them (see chapter 5.4).
Approval module	Here you can see all modules that have been activated for you on the Aareal Portal. Contact your Aareal client advisor to modify the selection of activated modules. An overview of all the modules available on the Aareal Portal can be found on page 15 in chapter 4.2 of the User Manual. If the function for displaying and using accounts held with other banks in the Aareal Portal has been activated for you, you will see the words **With link to third-party bank**.

Table 1: Master data for client logon

Beneath the master data, all active and inactive users of your client logon are listed in the table entitled **Client's users**. This is where you can set up new users, lock or delete existing users (Status: “Terminated”), reset passwords and define roles, modules and account restrictions for users.

> ! ***NB**: When you make any changes to an existing user or set up a new one, remember to store this by clicking on* **SAVE** *at the bottom of the table. Otherwise your settings or updates will be lost.*

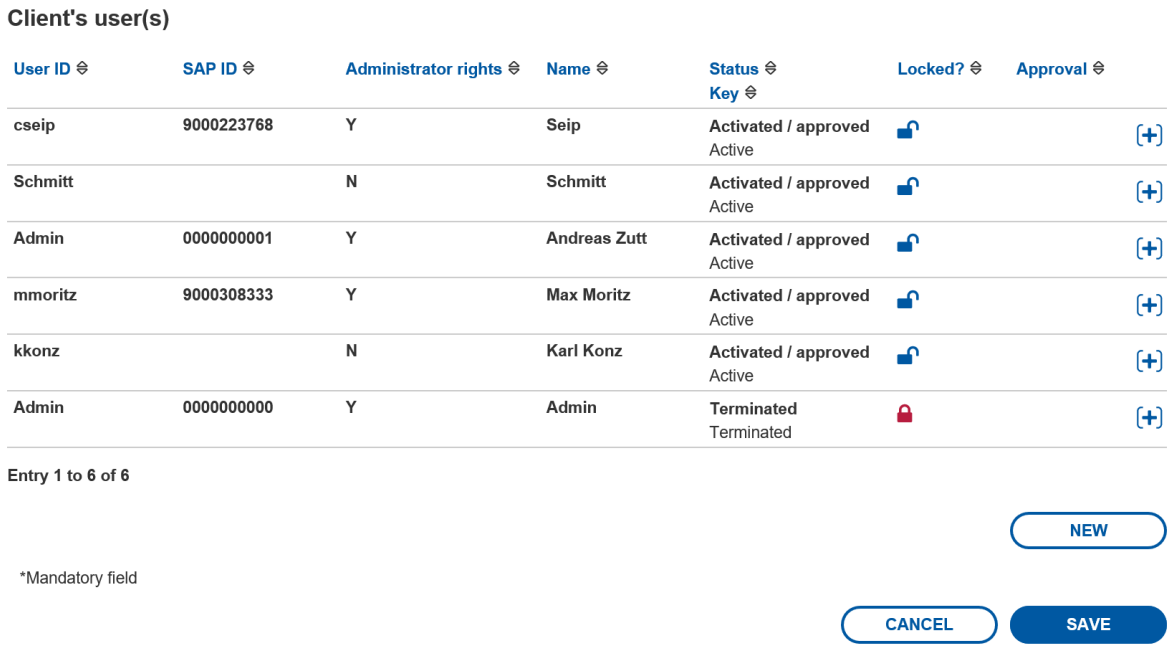

Figure 2: Client's users

The **User ID** is the unique identifier for a user within your client logon. The user logs onto the Aareal Portal by utilising the user ID, the client ID that you have defined above plus a password freely selected by the user. The user ID is also displayed in other parts of the Aareal Portal, e.g. in the logs.

An **SAP ID** is only defined for users with administration rights. The letter "Y" in the **Administrator rights** column indicates whether these rights have been assigned. If you want to set up a new user with administration rights, please contact your client advisor at Aareal Bank, who can also assign administration rights to an existing user or revoke them.
To assign administration rights, your client advisor will require an SAP ID and the user's full address.

The **Name** column shows the user's full name.

The next column shows you the **Status** of the user ID and the **Key** assigned to the user in question.

The following statuses are possible for the user ID:

Created	A new user ID has been created. No logon data have been generated or sent at this stage.
Logon data dispatched/created	Logon data have been requested for this user ID after a new user has been created, an existing one has been locked, the password has been forgotten or for other reasons. The user has not yet logged on with his or her initial logon data.
Activated / approved	This is the basic status for an activated user ID. The user can work on the Portal.
Locked	The user access has been locked as a wrong password or TAN has been entered three times or as a result of a deliberate action. Depending on the cause of the lock, the imageTAN reader must be re-activated and new EBICS keys generated.
Terminated	A terminated user is permanently deactivated and cannot be re-activated. The user is still listed in the table for information purposes.

Table 2: Possible user ID statuses

The following key statuses are possible:

Status	Description
Active	The key has been activated and is linked to the user ID.
Awaiting approval	The key has been activated by the user and is awaiting approval by the administrator. This is where you enter the approval code that you receive back from the user. Further information can be found in chapter 5.5. This status is only used if the option "Key requires approval" has been selected in the **Key** tab when creating the user.
Unknown	The key has not yet been activated. No key has been linked to the user ID or the link has been cancelled, e.g. because the user has been locked.

Table 3: Possible key statuses

The "**Locked?**" column shows you whether a user is currently locked or not. Locked users are designated by a closed red lock. Non-locked users are denoted with an open blue lock.

You can find out more about locking and unlocking users in chapter 5.2.

Approving users

If users are set up or changes are made by an administrator at Aareal Bank, they must be approved by a second administrator at Aareal Bank in accordance with the "4-eyes principle". This procedure ensures that administrative errors are avoided.
If approval has not yet been given by the second administrator, this is indicated by the words "Waiting for approval" in the **Approval** column. In addition, the entire line is

highlighted in grey. Any changes to the user do not take effect until they have been approved by the second administrator.

In your role as the administrator of your client ID you are not subject to the "4-eyes principle" in connection with the activation of your employees. Any changes that you make to your users take effect immediately after you click on **SAVE**.

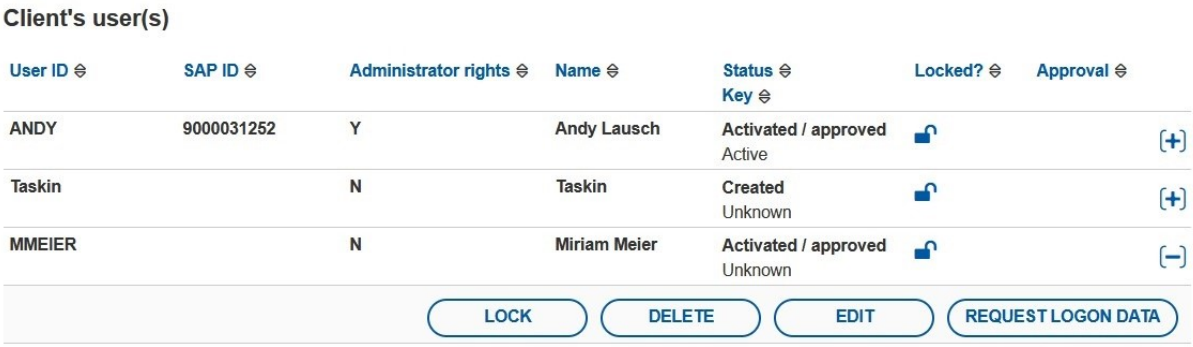

Figure 3: Actions for locking, deleting, editing users and for requesting new logon data

Clicking on **[+]** at the end of a user entry line will give you access to actions that you can perform on the individual users. Specifically, these are as follows:

- You can temporarily **LOCK** a user. In this case, the user's settings and data including any existing EBICS keys are retained. A lock takes immediate effect. To remove a lock, use the button **REQUEST LOGON DATA** and commence the approval process.
- Click on **DELETE** to permanently delete the user.
  A deleted user permanently remains listed in the **Client's user** table for information purposes (Status: “Terminated”). It is not possible to re-activate the user.
  If the user is still linked with an active imageTAN reader, the licence for the imageTAN reader in question is automatically released. This deactivates the imageTAN reader, meaning that it can now be activated and used by another user.
- With the **EDIT** button you can modify all data, rights, restrictions etc. of a user. Please note that any changes that you make to the user are not effective until you click on **OK** on the editing page and also click on **SAVE**. If you don't do this, the changes will be discarded, meaning that you will have to enter them again.
- Clicking on **REQUEST LOGON DATA** lets you have the user set a new password at any time, e.g. after you have set up or locked the user. Further information can be found in chapter 5.4.

5.1. Setting up a new user or modifying an existing one

To set up a new user, go to **USER** in the **MANAGEMENT** module and click on **NEW** at the bottom of the page.

If you want to modify the data, roles or restrictions assigned to an existing user, you also open this page to manage users under **MANAGEMENT ▶ USER.** Then select the user in

question from the table, open the action menu by clicking on **[+]** and click on **EDIT**. Alternatively, you can simply click on the line containing the user in question.

This will open the **Edit user** page with four tabs. The following section describes the procedure for setting up a new user. Where there is a different process for editing existing users, this is expressly stated.

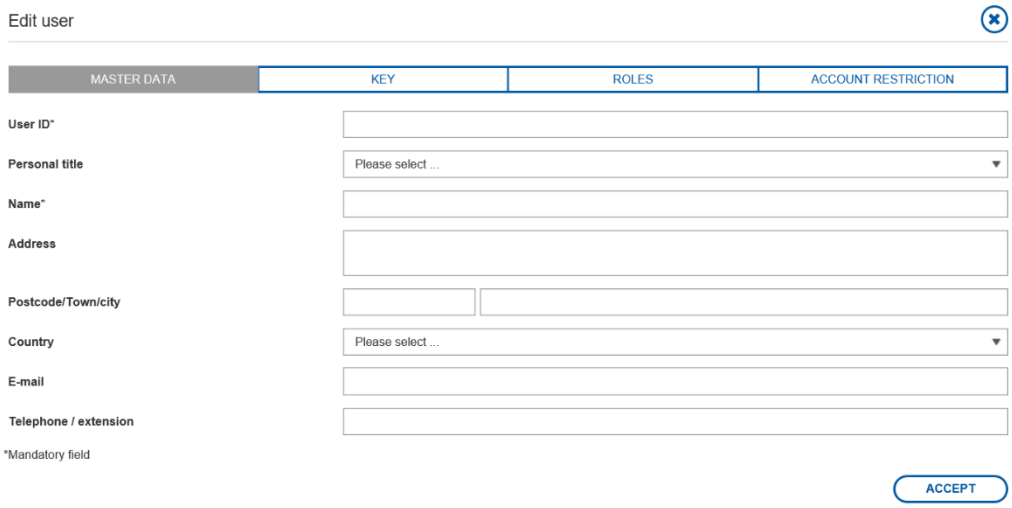

Figure 4: Setting up a new user – entering the master data

First you enter the user's personal data in the **Master data** tab.

The **User ID** is the unique identifier of this user in your client ID for the Aareal Portal. The user logs onto the Aareal Portal with this user ID, the client ID and his or her password. However, the user ID is also required for logging purposes and for assigning imageTAN readers to users.

You are free to choose any user ID. However, a User ID must be unique, i.e. it must not already exist within your client logon. It can have a length of up to 100 characters.

! **NB**: *It is advisable to use what from your point of view is a meaningful system for assigning user IDs so that you can quickly identify the individual users. Select a user ID that is easy to remember as the user must enter it whenever he or she logs on.*

Under **Name**, you enter the user's full name. This name is used in different places on the Aareal Portal to address or identify the user. Thus, the name of the user is displayed in the top right corner of the portal whenever he or she is logged on, in various logs as well as in the user ID activation letter.

You must enter at least a **User ID** and **Name** for the user. Then click on **ACCEPT** to add the user to the user list. When the dialog has been closed, make sure you click on **SAVE** to complete the procedure and save the new user.

In most cases, it will also be helpful to complete the remaining fields. This will assure you of updated information if you or other administrators need to contact the user at a later date, e.g. to provide assistance.

The full **Address** including **Postcode**, **town/city** and **Country** are inserted in the activation letter. If you want to send the letter by ordinary mail, it is a good idea to insert a valid address here.

A valid **E-mail** address is necessary so that the user can set up the notification function in the mail box.

The next tab, **Key**, is used to set up the user's key.

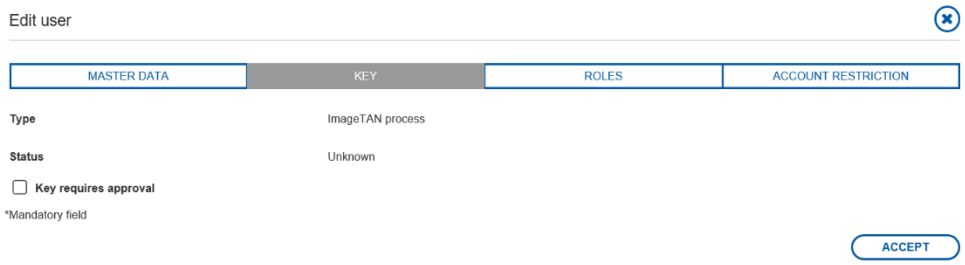

Figure 5: Setting up a new user – setting up the key

The **Type** "imageTAN process" is the default setting and describes the logon procedure using the imageTAN reader as a key.

Status indicates one of the possibilities shown in Table 3: Active, Awaiting approval or Unknown. This status is also shown in the **Key** column of the **Client's users** table.

Tick **Key requires approval** if you want to approve the user manually. In this case, the user will be given a letter setting out an approval code for downloading as soon as he or she has activated his or her imageTAN reader and will be asked to forward it to you. The user cannot log on until the code has been verified by you. This additional step for approving users is described in detail in chapter 5.5.

! **NB:** *The key for an administrator logon always requires approval. This approval must be given by Aareal Bank.*

If a key has already been activated and approved, you have the possibility on the right-hand side of the screen to revoke this activation. Figure 6 shows how this is done. Click on the icon with the counter-clockwise arrow to reset the key and to deactivate all digital keys for all banks connected to it. You must re-activate the user so that he or she can log onto the Aareal Portal again.

! **NB:** *Please contact your client advisor at Aareal Bank to revoke the key attached to an administrator logon.*

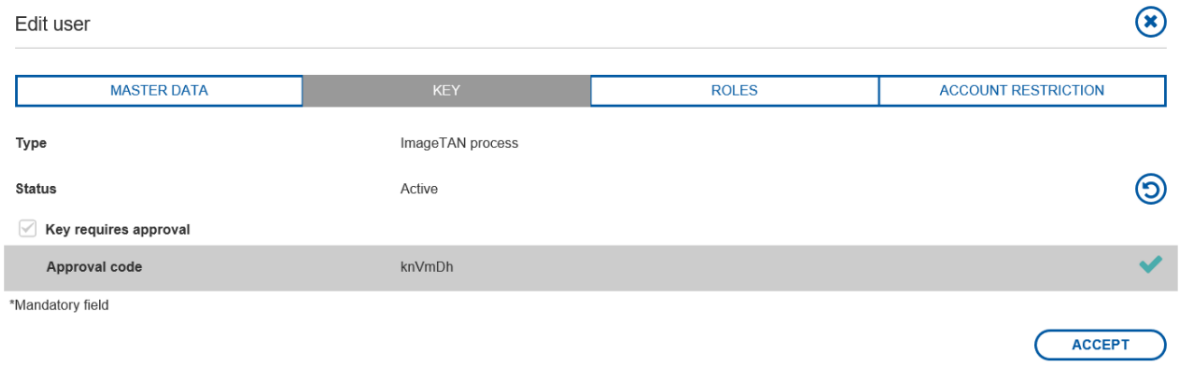

Figure 6: An activated key with the possibility of revoking it

The next tab is entitled **Roles** and lets you determine the information that users can view or edit.

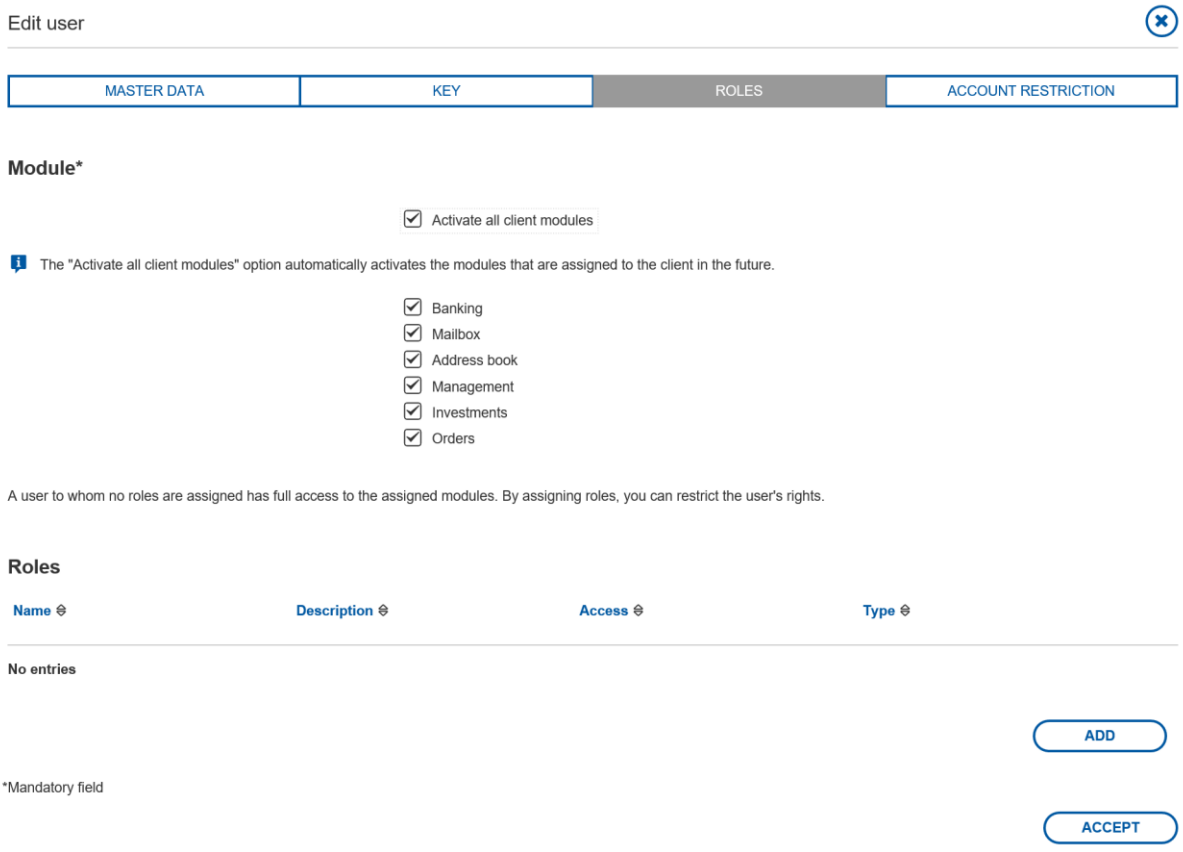

Figure 7: Setting up a new user – Selecting modules and defining roles

The default setting is for the user to have access to all client modules that are currently activated. As you can see in Figure 7, all currently available modules are preselected. If you want to automatically activate the user for all modules that will be added to the Aareal Portal and activated for you in the future, tick **Activate all client modules**. This alleviates you of the need in the future to change the settings for all users who are permitted to access all parts of the Aareal Portal.

This means that the user can access all functions in all the modules you have selected except if you make any other changes. Modules that are not required for the user can be deactivated by unticking them. These modules will then no longer be visible to the user on the Aareal Portal. You can assign roles to the user to additionally restrict the functions available to him or her.

> **!** **NB:** *For users without any administration rights (see Figure 2), the* **MANAGEMENT** *module includes functions for changing their own password, for managing their own EBICS keys, for carrying out retrievals in the retrieval manager and for viewing the logs. Users do not automatically have access to administrative functions such as user management, the management of roles and rights or the imageTAN reader. These functions are only visible to users who hold administration rights.*

Click on **ADD** and select one or more roles that you want to assign to the user.

The scope of the functions available to a user in the Aareal Portal is the sum total of all authorisations under the roles assigned to him or her.
If, for example, a role stipulates that a user has reading rights for the mailbox and another role also assigned to him also gives him or her writing rights for the mailbox, the higher rights, i.e. the writing rights, will always apply.

Chapter 6.1 tells you how to set up further roles.

In the last tab entitled **Account restriction**, you can determine the accounts which a user is permitted to access. Details on the possible configurations can be found in chapter 6.2.

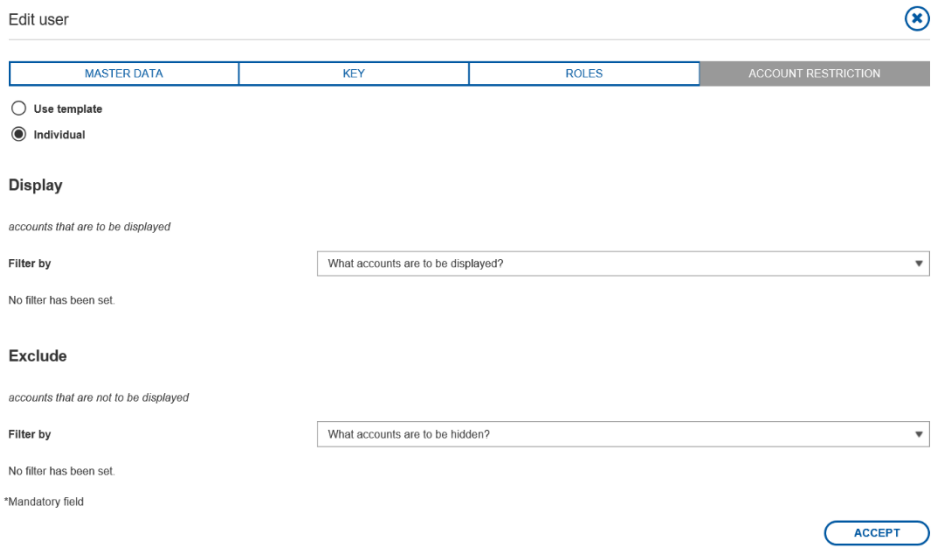

Figure 8: Setting up a new user – Defining account restrictions

As soon as you have entered all the necessary data, you can import the user data to the user management function by clicking on **ACCEPT**. Remember to click **SAVE** to store your changes and complete the process.

The new user has now been set up and assigned "Created" status. However, the user requires the initial logon data to log on. Please follow the instructions set out in chapter 5.4 to issue this information.

5.2. Locking users

Locked users cannot log onto the Aareal Portal and are shown a notice to this effect on the logon page.

Click on LOCK below the user entry to lock the user. If you want to unlock the user again, click on REQUEST LOGON DATA to initiate the activation process that is also used for new users. Needless to say, the blocked user's settings and data are still available.

! **NB**: *When a user is locked, it is not necessary to click on SAVE to store the changes as the action takes effect immediately. If the user is logged on at that precise moment, the session is terminated and he or she is logged off.*

! **NB**: *You can also lock your own administrator logon. If you have not set up any other administrator logon, this will mean that you are temporarily unable to manage the Aareal Portal. In this case, please contact your client advisor at Aareal Bank so that you can be reactivated.*

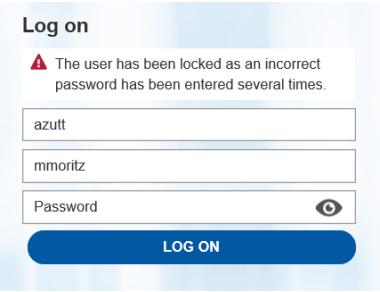

Figure 9: Warning message for locked user

For security reasons, two different locking levels have been implemented for the Aareal Portal:

A user who enters an incorrect password three times or has been sent new logon data - e.g. because he or she has forgotten his or her password - can continue working on the Aareal Portal immediately after setting a new password. His or her imageTAN reader remains activated.

If a user has been locked as a result of any of the activities set out below, the licence of the imageTAN reader is revoked and the reader is deactivated. In addition, the keys for the user's EBICS participant ID are deleted. This means that after being assigned a new password, the user must take the corresponding steps again to activate the imageTAN reader and to generate new EBICS keys.

Actions resulting in the deactivation of the imageTAN reader licence and the EBICS keys are:

- entering the wrong TAN three times
- clicking on the LOCK IMAGETAN READER button on the logon screen
- deactivating the reader on the imageTAN reader management page

5.3. Setting up an additional administrator

It is advisable for various reasons to assign administrative tasks to multiple persons. These include improved availability, distributing workloads and ensuring fill-in arrangements in the event of illness and vacation.

A further important aspect is the fact that an individual administrator may inadvertently lock himself or herself out of the Aareal Portal by forgetting his or her password or repeatedly mistyping the password. Obviously, your client advisor at Aareal Bank will be happy to help in such cases by resetting your password.
However, by setting up a second user with administration rights, you remain fully operational and independent in such a situation and are more readily able to reset the user ID.

Your client advisor will be happy to set up further users with administration rights for you. So please feel free to ask.

5.4. Assigning new logon data to a user

There are various situations in which it may be necessary to assign new logon data to a user.

- You have set up a new user in accordance with chapter 5.1 and want to send him the initial logon data.
- You want to unlock a previously locked user.
- A user has forgotten his or her password or entered an incorrect one three times. You now want to send him or her a new (initial) password.

As the administrator, you will never be able to view or modify a user's password. This security feature ensures that actions that can be traced to a user in the activity log (see chapter 10) can be reliably tracked back to that user. After all, only the user himself knows the password for his or her user logon at any given time.

Click on **REQUEST LOGON DATA** on the user management page to create a new initial password for the user, which is available for downloading as a PDF file. Please send this document to the user.
The previous user's password becomes void upon new logon data being requested.

With the information contained in the letter the user is able to log on to the Aareal Portfolio again or for the first time as the case may be. He or she is prompted to select a new password during the logon process. After this has been done, the status is set to "logon data sent/generated".

The imageTAN reader is activated at the same time as the completion of the initial logon process. This is done by scanning the initialisation image TAN and is described in detail in chapter 3.

If a user has forgotten his or her password and therefore requires new logon data, the imageTAN reader remains activated. Similarly, all keys for the EBICS participant IDs assigned to the user are retained and do not have to be generated again.

5.5. Key activation by the administrator

If you like, you can determine that you as the administrator must manually approve the keys. This gives you as the administrator more control over the point in time at which you activate a user and generally ensures greater security in activating new users.

! **NB:** *The key for an administrator logon always requires approval. This approval must be given by Aareal Bank.*

To set the key so that it requires approval, open the screen for setting up a new user or for editing an existing one, as described in chapter 5.1. Then click on the second tab entitled KEY and tick **Key requires approval**.
Remember to ACCEPT the changes and then SAVE them on the user management page.

After activating the imageTAN reader, the user is offered a "Document for imageTAN activation" for downloading and must forward this to you. This step is described in chapter 3, figure 6 of the User Manual.

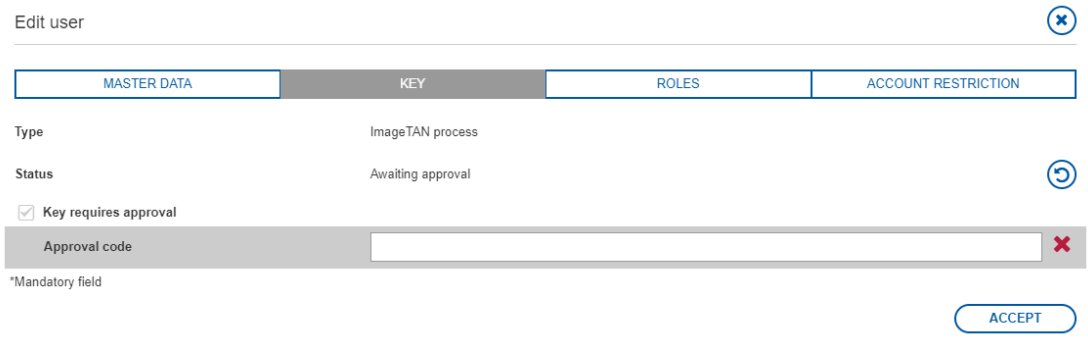

Figure 10: Approving a key with an approval code

Enter the approval code that you have received from the user in the activation letter in the KEY tab of the Edit user screen. As soon as the code has been accepted, a green tick is displayed to the right of the input field. Confirm the changes by clicking on ACCEPT and SAVE them on the user management page.

The user is now activated.

If the user has forgotten to download the document or if the document has been lost, please click on REQUEST LOGON DATA to have the user go through the initial logon process again.

5.6. Changing your own password

The password that you currently use to log onto the Aareal Portal can be changed at any time. The option is available to every user of the Aareal Portal.

To do so, open the Management module and then the menu item "Profile". You are automatically taken to the dialog to change your password:

MANAGEMENT ▶ PROFILE ▶ CHANGE PASSWORD

In the next dialog, please enter your current password followed by your new password. An indicator gives you a sense of the complexity and thus the security of your new password.

> ***Note**: In the interests of greater security, please choose a password that you use solely for the Aareal Bank's Portal.*

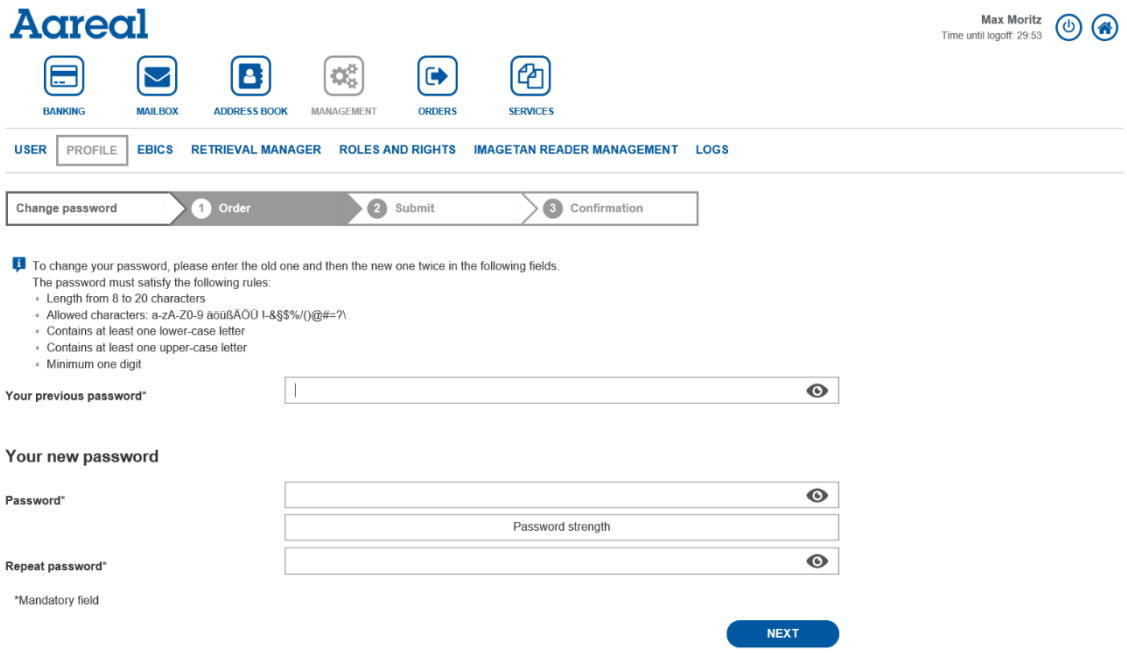

Figure 11: Changing your own user password

If you have forgotten your previous administrator password, please contact your client advisor at Aareal Bank, who will arrange for you to receive new initial logon data as quickly as possible.

6. Roles and rights

Not all users should be able to access all the functions available on the Aareal Portal and all your account data. Accordingly, the Aareal Portal offers two options for restricting access to your content:

Using roles, you can combine pages on the Aareal Portal that employees require to perform typical activities. For example, you can grant an employee who is responsible for bookkeeping activities access to the financial status and the mailbox, but not grant him or her the right to execute payments. Another employee could initiate transfers and direct debits but is not authorised to perform any foreign payments.

As the tasks vary within your company, you can define roles in line with your requirements. You can then assign each role to one or several users. If you assign a user more than one role, the rights involved will be aggregated.

If you have set up several accounts in the Aareal Portal and don't want to give all users access to all accounts, you can limit their reading rights by means of account restrictions.

Here, too, you define Portal-wide restrictions which you can then assign to individual users.

Please refer to chapter 5.1 above to find out how to assign roles and account restrictions to users. The following chapters explain how they are set up and managed.

6.1. Setting up and managing roles

Open the Management module and then click on Roles and Rights in the menu.

MANAGEMENT ▶ROLES AND RIGHTS ▶DEFINITION OF ROLES

This will display a list of all the roles available to you. Even if you have not yet defined any roles of your own, the following minimum role definition is available:

- **Account inspection for third parties** allows the user to view the account transactions stored on the Portal.

In addition, your administrator at Aareal Bank may have defined roles that you can also use. More details can be found further down in the chapter.

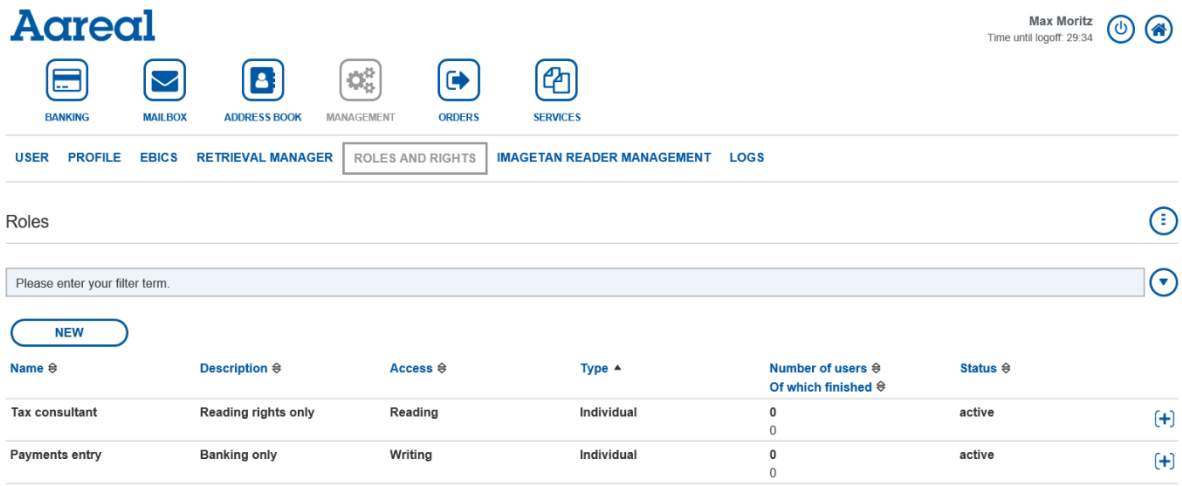

Figure 12: Overview of the existing roles

To define a new role, click on NEW in the top left corner. This displays the page, a part of which is shown in Figure 13.

First assign a **Name** and then a **Description** which reflects the purpose of the role for you and other administrators.

You can also restrict the role by ticking **Reading rights only**. If this box is ticked, the user to whom this role is assigned only has reading rights for the pages selected lower down.

If you want to assign a role with mixed reading and writing rights, please define two roles and then assign both of them to the user. All roles assigned to a user are aggregated. This means that the higher right always overrides the lower one:

For example, if a user is assigned reading rights for the signature folder in one role and writing rights in a second role, this means that he or she has writing rights for the signature folder.

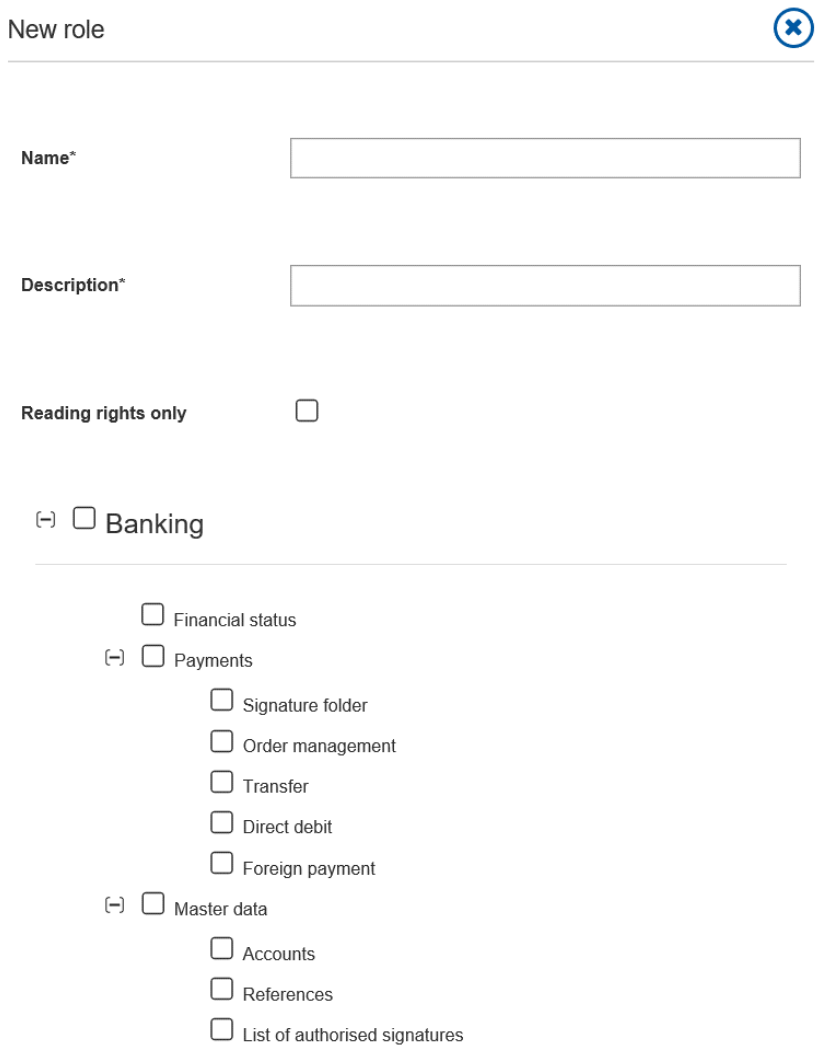

Figure 13: Extract from the page for defining a new role

Now select the screens of the Aareal Portal which you want to make accessible to the holder of the role. In the mailbox section you can also assign individual directories. It is a good idea to set up these directories before you define any roles. Otherwise, you must remember to include any new directories in the definition of the corresponding roles.

Store the new role by clicking on **SAVE** in the bottom right-hand corner.

The new role will now be displayed in the **Roles** table.

The Access column states whether the role grants **reading** or **writing** rights.

Type indicates whether you have defined the role yourself ("Individual") or whether it has been provided by the administrator at Aareal Bank ("Standard"). Please note that you can only edit or delete rights that you have defined yourself.

Number of users shows how many users are utilising the role in question. This information is important to determine whether you can edit a role definition during ongoing operations.
In the line below ("**Of which finished**"), you can see how many users have been terminated and are therefore no longer permanently active.

Status shows whether the role is still active or has been deleted. You can delete individual roles by clicking on **[+]** in the corresponding line and then on the **DELETE** button.

Role definitions that have been deleted cannot be reactivated. They are retained in the Aareal Portal (Status: “Terminated”) so that they can be tracked at a later date. For this reason, the same name cannot be assigned more than once.

Deleted role definitions are hidden by default settings. If you want to view them, click on **ADVANCED SEARCH** next to the Quick filter input field and select "Deleted" in the **Status** field. After confirming with **FIND**, you will see all deleted roles.

6.2. Setting up and managing account restrictions

Using account restrictions, you can determine what viewers can view what accounts. The procedure is similar to that for defining roles: as the administrator, you define the templates for account restrictions and then assign them to one or more users. Alternatively, you can define account restrictions in the final tab of the editing page for individual users. In this case, the account restrictions apply only to that user.

If you want to work with other banks in addition to Aareal Bank on the Aareal Portal, you must set these up before you define any account restrictions.

Open the Management module and then click on Roles and Rights in the menu.

MANAGEMENT ▶ ROLES AND RIGHTS ▶ ACCOUNT RESTRICTION

This will display a list of all the account restrictions available to you. The list is empty when you access the Aareal Portal for the first time.

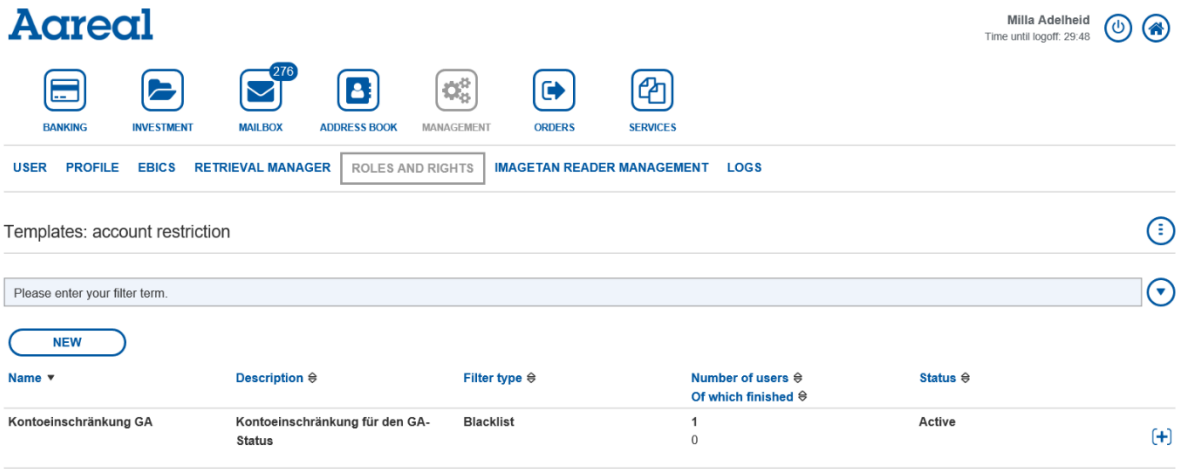

Figure 14: Overview of your account restriction templates

To define a new template for an account restriction, click on **NEW** in the top left-hand corner. This opens the dialog shown in Figure 15.

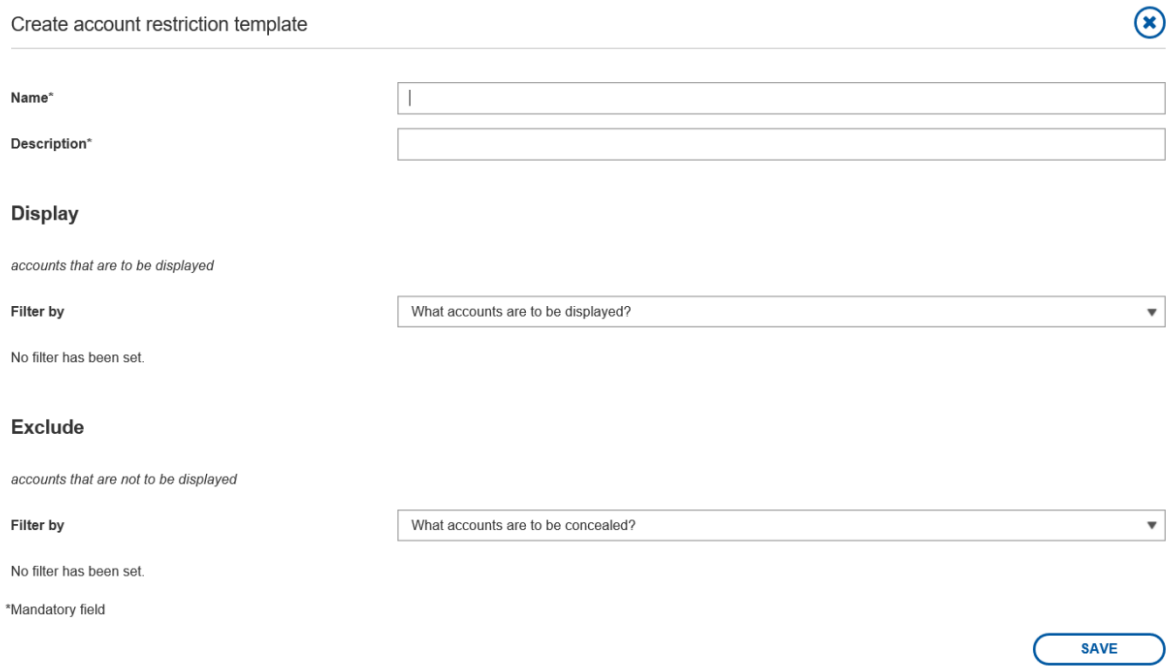

Figure 15: Page for defining a new account restriction

First assign a unique **Name** and then a **Description** which signifies the purpose of the account restriction for you and other administrators. These two designators allow the account restriction to be clearly identified and tracked later on.

As long as no account restrictions have been defined and assigned to users on the Aareal Portal, a user can view all the accounts set up on the Aareal Portal. You have two options for displaying account restrictions:

- You can set up a positive definition to state which accounts are to be expressly accessed. As soon as a user is assigned one of these "whitelist" account restrictions, all accounts that do not match one of these whitelist definitions are hidden.

  For example, you can define an account restriction which allows the user to access all accounts named "Notice deposit account". This restriction (and any other restrictions that may have been assigned to the user) would hide all accounts that do not match this definition.

- Alternatively, you can set up negative definitions to expressly exclude accounts. These "blacklist" restrictions show the user all accounts that do not match the restriction.

In addition, you are able to combine these two types of definitions. For example, you could define a restriction which grants the user solely access to "notice deposit accounts", with the exception of the account(s) that you expressly stipulate.

Obviously, you can also define account restrictions separately and combine them by assigning them to a user.

Whitelist restrictions are defined in the input fields in the **Display** areas:

Select one of the selection criteria from the **Filter by** list:

- Account number (IBAN)
- Account system ID
- Banks (BIC)
- Account holder
- Trustor
- Account name

In the following **Filter** section, you enter the value you want to filter by and confirm it by clicking on **+** to the right. In this way, you can enter and add further filters; the criteria are displayed in the list below.

! ***NB***: *You can only set one filter criterion per account restriction.*

If you want to remove any criteria, mark the corresponding entries and click on **DELETE MARKED ENTRY** or reset the entire filter by clicking on **RESET FILTER.**

To enter a blacklist account restriction, use the input fields in the **Exclude** section:

The **Filter by** selection list currently only offers you the option of hiding individual account numbers. Enter one or several IBANs as described in the **Display** section.

Then click on **SAVE** to store your settings.

The newly defined account restriction will now be listed in the **Templates: Account restriction** table shown in Figure 14.

Either **Whitelist** or **Blacklist** will be displayed in the **Filter type** column depending on whether you have defined the filters in the **Display** or **Exclude** section. If you have entered filter criteria in both sections, the filter type is set to **Combined**.

Number of users shows how many users are utilising the account restriction in question. This information is important to determine whether you can edit the definition of an account restriction during ongoing operations.
In the line below ("**Of which finished**"), you can see how many users have been deleted and are therefore archived.

Status shows whether the account restriction is still active or has been deleted. You can delete individual restrictions by clicking on **[+]** in the corresponding line and then on the **DELETE** button.

Account restrictions that have been deleted cannot be reactivated. They are retained in the Aareal Portal (Status: “Terminated”) so that they can be tracked at a later date. For this reason, the same name cannot be assigned more than once.

Terminated definitions of account restrictions are hidden by default settings. If you want to view them, click on **ADVANCED SEARCH** next to the Quick filter input field and select "Terminated" in the **Status** field. After confirming with **FIND**, you will see all terminated account restrictions.

7. ImageTAN reader management

In the interests of maximum security, the Aareal Portal requires a newly generated TAN to be entered in addition to your password whenever you log on as well as for financial orders to the bank. This TAN proves that you are the legitimate user and that you hold a registered key in addition to your valid password.

The imageTAN reader generates the TANs that you require. To this end, you scan the image displayed on your screen and then enter the TAN displayed by the imageTAN reader on the Aareal Portal. The imageTAN reader is tied to your specific logon and can only generate TANs for it. This prevents any unauthorised use by third parties.

This chapter describes all the functions on the Aareal Portal and the imageTAN reader that you require for your work as an administrator.

7.1. Viewing and approving activated imageTAN licences

In order to gain an overview of all currently activated licences being utilised by users - and hence the imageTAN readers in operation - open the following pages in the Management module:

MANAGEMENT ▶ IMAGETAN READER MANAGEMENT

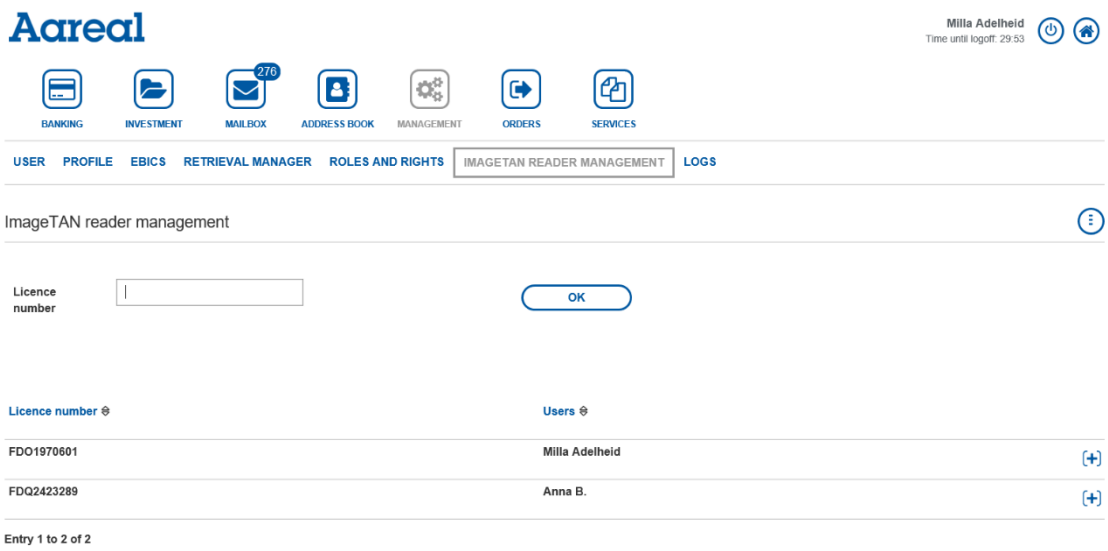

Figure 16: Overview of all activated imageTAN readers

The table lists all the **licence numbers** of the imageTAN readers being actively utilised by the individual **users.**

You can search for a specific licence by entering the licence number at the top of the page and then clicking on **OK**.

If a user has lost his or her imageTAN reader, you can deactivate it by withdrawing the licence. Click on [+] in the line of the corresponding user and then on **RESET IMAGETAN READER**. Answer [Yes] to the confirmation prompt.

When you reset the reader, all the EBICS keys assigned to this user will be deleted. Similarly, the user's PIN will also be deleted. The imageTAN reader can now be assigned to a new user.

The following chapter 7.2 explains how to display the licence number of an imageTAN reader that has been found or returned.

7.2. Editing the imageTAN reader settings

Each imageTAN reader has a configuration menu. You access this menu by switching off the device and holding down the on/off button at the top edge of the device for at least three seconds.

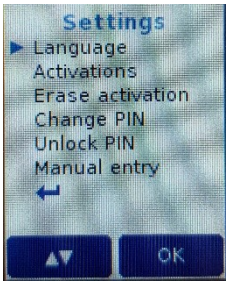

Figure 17: ImageTAN reader Settings

You see a **Settings** menu with the options shown in Figure 17:

- Select **Language** to choose the appropriate language for the user.

- **Activations** displays the currently used licence number, provided that the reader has been activated. If you find a reader or cannot clearly assign it to a user, you can find out the licence number by going to **MANAGEMENT ▶ IMAGETAN READER MANAGEMENT** to identify the user and, if necessary, deactivate the licence. Further information can be found in chapter 7.1.

- The menu item **Erase activation** deletes the active licence number from the reader. This function is additionally secured by enquiring the device PIN. Following this, the device can no longer be used for logging onto the Aareal Portal or for payments.

  ! **NB**: *Please note that the licence number is still assigned to the user on the Aareal Portal. It has merely been deactivated in the imageTAN reader. Reset the imageTAN reader for the user as described in chapter 7.1.*

  Use this function if, for example, the imageTAN reader is still registered for a previous user who has already been deactivated.
  The main way of deactivating an imageTAN reader is to follow the procedure described above in imageTAN reader management. However, it is also possible to click on the link entitled "Lock imageTAN reader?" (see Figure 18) on the Login page. In this case, you - as an administrator - should use the link for revoking the key in the **KEY** tab on the page for editing the user (see Figure 6).

- Via **Change PIN** the user can change the PIN that he or she has chosen for the imageTAN reader at any time. Refer to chapter 7.3.1 and chapter 7.3.2 to find out how to set a new PIN if you have forgotten the current one.

- **Unlock PIN** allows you to set a new PIN if you have forgotten the old one and the reader has been locked after a wrong PIN has been entered three times.

- The final setting **Manual entry** currently does not have any function but will be used in the future.

7.3. Remedying error situations

7.3.1. The user has forgotten his or her PIN

A user who has irretrievably forgotten his or her PIN can reset the PIN by clicking on the link "PIN forgotten or locked?" on the login page (see Figure 18). The precise procedure is described in chapter 7.3.2.

However, the user needs to know his or her password to access this input screen. If the password has also been forgotten - e.g. due to an extended period of inactivity - you must request new logon data for the user in accordance with chapter 5.4.

Another option for you as the administrator is to reset the user's imageTAN reader on the Portal. To do this, select RESET IMAGETAN READER in IMAGETAN READER MANAGEMENT. Details can be found in chapter 7.1.

! **NB**: *When the imageTAN reader is locked, all EBICS keys are also reset. They must be regenerated in accordance with chapter 6.2.3 of the User Manual.*

7.3.2. The user has locked his reader by entering an incorrect PIN

A user can only generate TANs with the imageTAN reader after entering his or her PIN. This PIN is freely selected by the user during the activation of the imageTAN reader.

A maximum of three attempts may be made to enter the correct PIN. After a total of three failed attempts - including after interruptions or after resetting the imageTAN reader - to enter the correct PIN, the PIN is locked. In this case, the reader displays the message "Your PIN has been locked. Please contact your administrator." Underneath this, a six-digit approval code is displayed.

The user can then unlock the reader himself or herself and set a new PIN. To do this, he or she logs onto the Aareal Portal as usual.

At the bottom of the login page there is a link with the words "PIN forgotten or locked?".

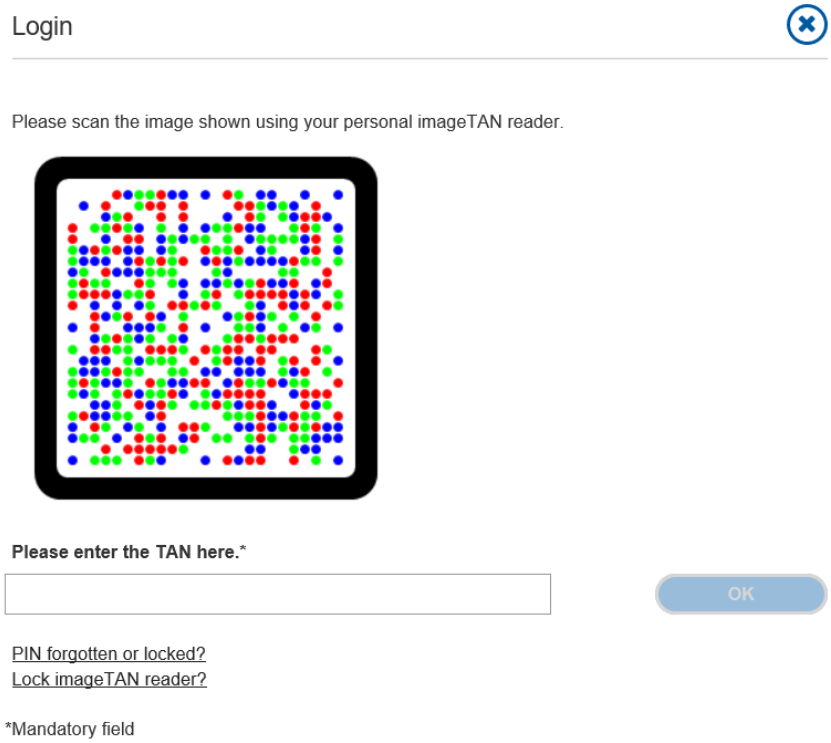

Figure 18: Login page

After clicking on this link, the user is prompted to enter the six-digit approval code.

The user must now enter the settings menu of the imageTAN reader as described in chapter 7.2. Then select **Unlock PIN** and enter the unlocking code on the Aareal Portal page.

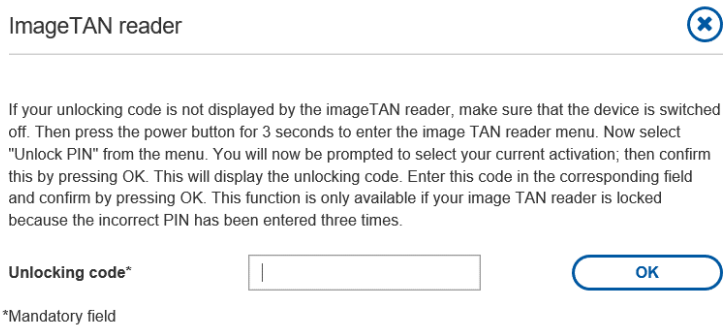

Figure 19: Unlock the imageTAN reader using the Unlocking code

The user is reminded that when a new PIN is set all EBICS keys will become void, meaning that he must be re-initialised with all banks. This must be confirmed by clicking on YES.

The next page shows the approval code to be entered in the imageTAN reader. If the reader has been switched off in the meantime, you must go back into the **Settings** menu and select **Unlock PIN** again.

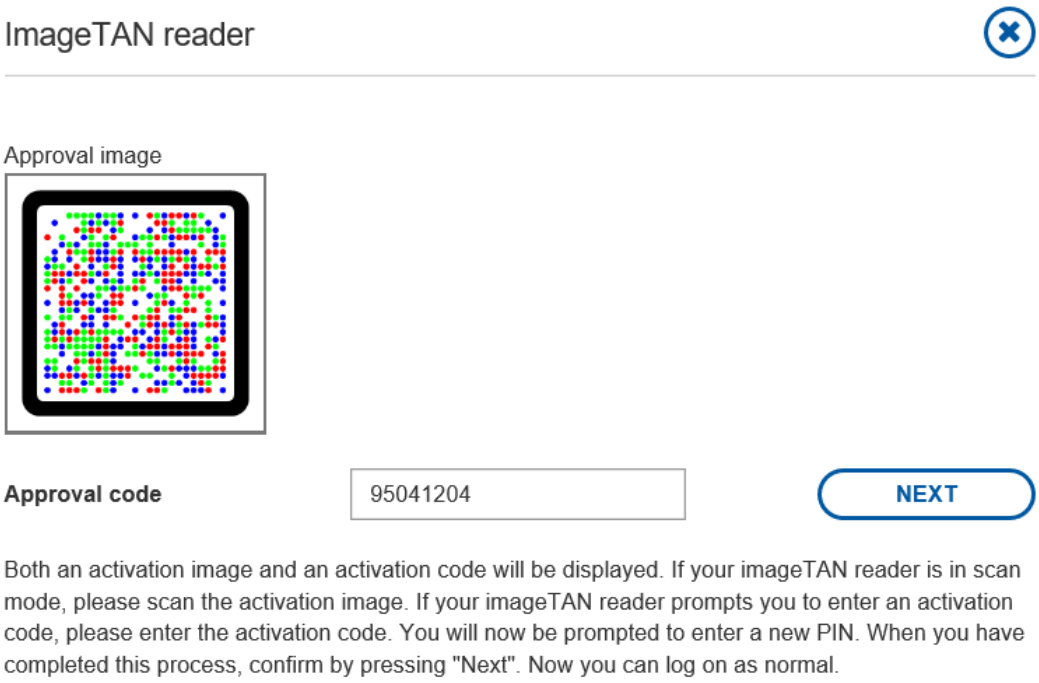

Figure 20: The approval code for entering a new PIN

Subsequently, a new PIN must be selected and entered twice. The user can now log back onto the Aareal Portal.

Please remember to generate new EBICS keys, as described in chapter 6.2.3 of the User Manual.

7.3.3. The user has lost his or her imageTAN reader

If a user discovers that he or she has lost his or her imageTAN reader, it is important for it to be locked as quickly as possible. This can be done either by the user himself or by you as the administrator on behalf of the user.

The user can lock the imageTAN reader by clicking on the link entitled "Lock imageTAN reader?" on the login page (see Figure 18). The user requires his or her logon data and password to reach this link.

Clicking on this link displays the confirmation prompt shown in Figure 21. It warns the user that his or her logon will be locked immediately and that all EBICS keys will be deleted.

To reactivate the user, send him or her a new imageTAN reader and follow the instructions shown in chapter 5.4.

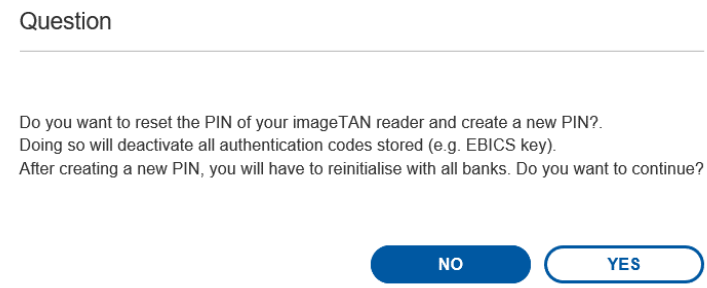

Figure 21: Confirmation prompt to lock an imageTAN reader

Alternatively, you in your role as the administrator can deactivate the user's imageTAN reader. This step also deletes all EBICS keys. Select the user in question in the menu **MANAGEMENT ▶ USER** , click on the user entry and then on the **KEY** tab. Now click on the small button with the counter-clockwise arrow to the right.

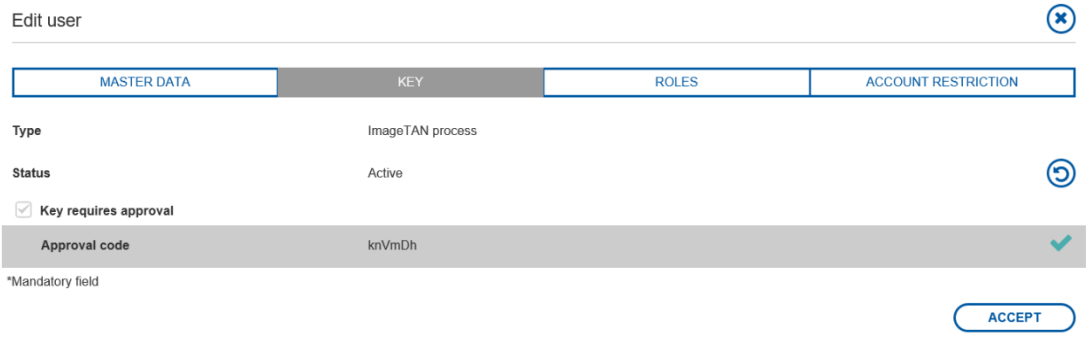

Figure 22: Deactivating an imageTAN reader in the Key tab

The user's previous imageTAN reader has now been deactivated and can no longer be used to log onto the Aareal Portal. The user can log onto the Aareal Portal with a new imageTAN reader. His or her Client ID, user logon and password remain valid. At the next login, the user is asked to reactivate his or her imageTAN reader. This is the same process as the one that applies to the initial logon. Then the user must re-initialise his or her EBICS keys.

Please contact your client advisor at Aareal Bank to deactivate an administrator's key.

7.3.4. A lost imageTAN reader is found again

To determine whether an imageTAN reader is assigned to a user, first identify the licence number stored in the reader. The procedure for this is described in chapter 7.2 in the **Activations** section**.**
Using the licence number stored in the imageTAN reader, you can now see the user to which the reader has been assigned in **MANAGEMENT ▶ IMAGETAN READER MANAGEMENT.**

If the device is not activated, i.e. no entry is displayed in the **Activations** section of the imageTAN reader, this means that the reader has not been assigned to any user. The reader is in its basic condition and ready for use.

If the reader has been assigned to a user and this user wants to continue working with the reader (e.g. because he or she has lost it), return it to the user. If the PIN has been locked for security reasons, it can be unlocked again via the link **PIN forgotten or locked?** (see Figure 18).
If necessary, remind the user to re-initialise his or her EBICS keys after unlocking the reader. The procedure for this is described in chapter 6.2.3 of the User Manual.

If an activated reader is returned to you and you are unable to identify the user, or the user is now using a replacement device and you want to delete the activation but don't know the PIN for the reader, please return the imageTAN reader to Aareal Bank.

8. Assigning EBICS participants to users

By logging onto the Aareal Portal, the user is able to access the data stored in the Aareal Portal. In order to be able to retrieve account transactions from Aareal Bank or another bank and to perform activities such as approving payment orders, the user requires corresponding EBICS rights from the bank in question. This chapter explains how to assign EBICS authorisations to users and manage these account rights.

If you are not yet familiar with EBICS authorisations, please refer to chapter 5.2 of the User Manual. Table 1 provides a brief overview of the available rights A, B, E and T.

To perform the following steps, you require preconfigured EBICS participants from all banks set up on the Aareal Portal. Please contact your client advisor if you don't have any EBICS participants.

In addition, the bank parameters for performing the following steps must already be configured. Please refer to chapter 6.2.1 of the User Manual for details.

Two steps are necessary to assign a ready-to-use EBICS authorisation to a user:

- First of all, an EBICS participant is allocated to the user. The EBICS participant defines the rights for accessing the accounts held with a bank. If a user is to be authorised to access accounts held with multiple banks, an EBICS participant must be assigned to that user for each bank.

  This step can either be performed by an administrator for all users, or a user can assign himself or herself EBICS participants.
  Later on in this chapter you will learn how to allocate EBICS participants to other users. However, if you want to assign yourself an EBICS participant, please refer to chapter 6.2.3 of the User Manual.

- In the second step, each newly allocated EBICS participant must be initialised. To this end, the imageTAN reader is used to generate keys for authenticating the user with the corresponding bank and for encrypting the communications. Each

user must do this personally. The individual steps are also described in chapter 6.2.3 of the User Manual.

Go to the Management module and open the page for configuring the bank parameters:

MANAGEMENT ▶ EBICS ▶ BANK PARAMETERS

Then click on the **[+]** symbol for the bank parameter for which you want to grant EBICS rights and click on **CHANGE**. This opens the **Detailed view of bank parameters** dialog. Now click on the last tab entitled **Participants**:

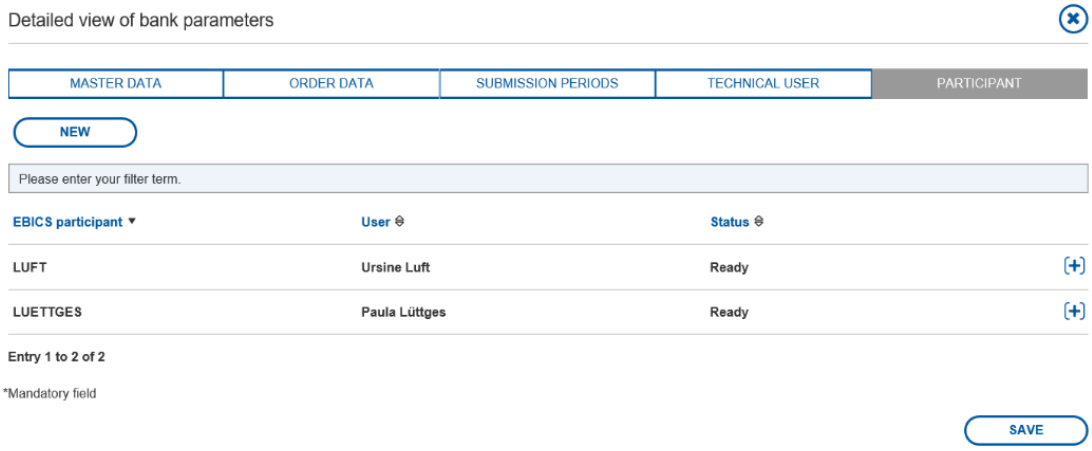

Figure 23: Allocation of EBICS participants to users

If you have already assigned EBICS participants to users, you can see these in the table.

Click on **NEW.**

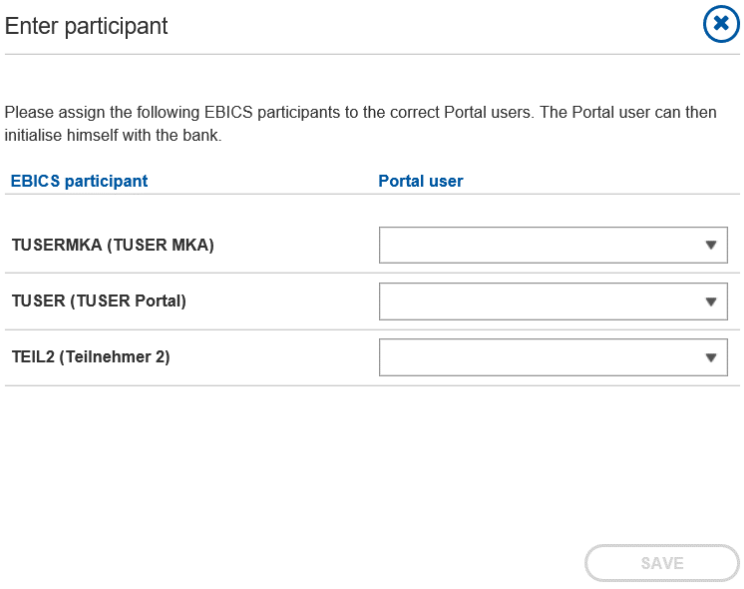

Figure 24: Assigning new EBICS participants to users

This opens the **Enter participant** page, the appearance of which varies according to whether the bank parameter for Aareal Bank or for another bank is displayed. In the former case, the names of the EBICS participants are displayed and merely need to be assigned to the relevant Portal users in the drop-down list in the column to the right. In the case of the bank parameter for another bank, the EBICS participant numbers must be individually entered before they can be assigned to the Portal users. Repeat this step until all users have been allocated and then **SAVE** your settings.

Now continue assigning EBICS participants to users for your other bank parameters.

Remember to subsequently tell your users how to initialise their EBICS participants. Chapter 6.2.3 of the User Manual describes the procedure for using the initialisation assistant.

9. Retrieval manager

Using the retrieval manager, you can obtain account statements, messages from your bank and other information and place these in the mailbox.

The retrieval manager is a function available to all Portal users. Retrievals can be configured by all users and are visible to all users. Similarly, retrievals of information stored in the mailbox or in the logs section can be performed by all users. Chapter 6.3 of the User Manual describes how the retrieval manager works.

If you decide to configure the retrieval manager centrally, you define roles to limit access to it. The precise procedure is described in chapter 6.1.

10. Activity logs

The activity logs document all important actions that you or a user managed by you have performed on the Aareal Portal. Examples include:

- User logons and logoffs on the Aareal Portal
- Setting up or deleting *EBICS* participants
- Preparing or signing payment orders
- Setting up mailboxes
- Setting up, editing or deleting mandates
- Setting up, locking or terminating users
- etc.

Activity logs can be viewed in the Aareal Portal for a maximum period of 24 months and will then be deleted. The deletion period may be shorter in some cases. You can access the activity logs via **MANAGEMENT ▶ LOGS ▶ ACTIVITY LOGS**.

In addition to the **date** and **time** of the activity performed, the log also displays details such as the reference number of the mandate and the EBICS participant.

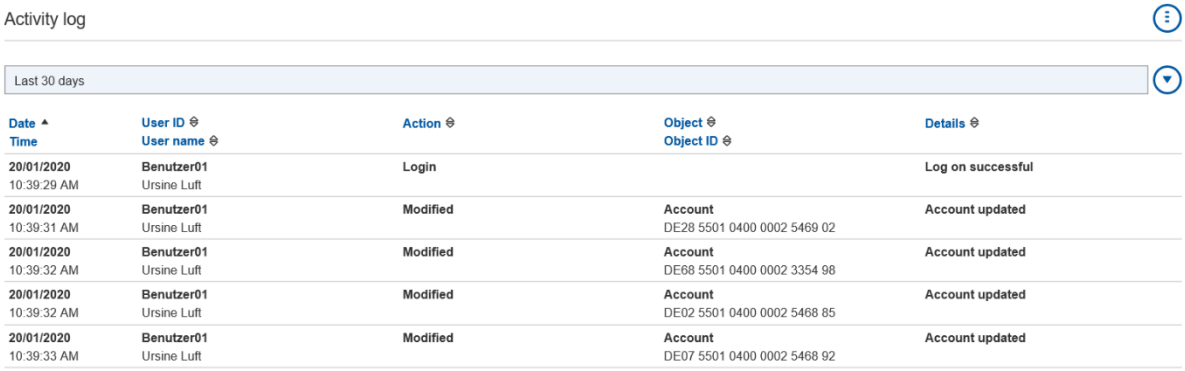

Figure 25: Activity log

Click on the individual line entry to obtain more information on the action in question. The following illustration shows detailed information on a newly created mandate.

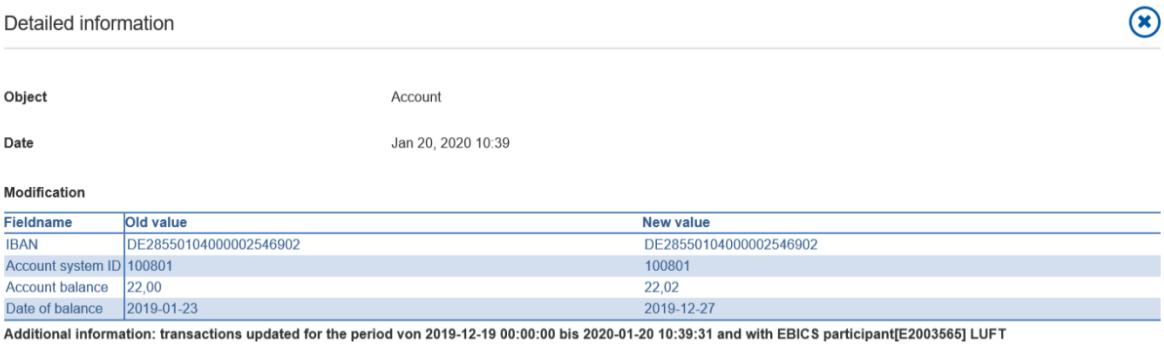

Figure 26: Further detailed information in the activity log, citing as an example a newly created mandate

! ***Note**: No detailed information (partner data) and thus GDPR-relevant data will be displayed in the log entries of the activity log for a partner who has been deleted from the address book.*

11. List of figures

12. List of tables