UIM User Guide

Version 3.0.4

Release date February 1, 2016

Table of Contents

1. Introduction

1.1. Purpose of document

This document is a user guide for end users who will use User Identity Management (UIM) to manage their identities. UIM is a simple tool for user and identity management and it is delivered as a standard part of ADUCID®. This user guide is intended for end users who can easily perform simple PC tasks—start and use basic user programs, such as web browsers.

The document provides PEIG® users with the following information:

- ADUCID® key terminology
- User's first log in via ADUCID®
  - Creating a cybernetic identity
  - Registering personal information and user authentication (optional)
    - Scenario 0—no registration
    - Scenario 1—registration using a pairing key
    - Scenario 2—registration using the registration form
    - Scenario 3—registration transferred from another provider
- Identity management in UIM
  - Changing, renewing, or removing an identity
  - Resolving operation issues (backup, loss, forgetting, or PEIG® malfunction)
  - Changing personal information
- Common questions about identity authentication and management

1.2. Supported systems

The UIM application currently supports the following operating systems and browsers.

Operating system	**Browsers**
Windows 7, 8	Internet Explorer, Firefox, Google Chrome
Android	Firefox, Google Chrome
OS X	Safari, Google Chrome
iOS	Safari, Google Chrome

2. ADUCID® key terminology

2.1. What is ADUCID®

ADUCID® is a new way for applications to authenticate users.

The main benefits of ADUCID®:

- Simple, secure and automated authentication
- Unified authentication, by using a single PEIG®
- Guaranteed privacy for users during the authentication process and through personal information management
- Authentication with a high level of security

2.2. PEIG®

A Personal Electronic Identity Guardian (PEIG®) is a device that can fully manage end-user cybernetic identities. Under a user's identity, it also provides automatic authentication between the client application and the application that the user is trying to access.

2.3. AIM

ADUCID® Identity Machine (AIM) is a software application operated by an identity provider. It manages authentication services between users, target applications and target systems. It also provides cybernetic identity services that are essential for authentication services. AIM can be managed via the User Identity Management (**UIM**) interface. The UIM application provides an easy way to manage identities and ADUCID® security parameter settings. UIM can be used for authentication to AIM by administrators, as well as by users themselves. The number of options shown depends on whether the end user is an administrator or a user.

2.4. Identity and related terms

Physical identity is an identity that is based on what we perceive through our senses.

Cybernetic identity (hereinafter also "identity") is a unique distinction of a particular PEIG® user, and it allows a particular user to access to electronic services. The essential part of user's cybernetic identity is stored on their PEIG®. The cybernetic identity is recognized by AIM, which is operated by the identity provider. Users can have any number of different cybernetic identities. Cybernetic identities are unique representations of a user in the cybernetic world and they contain no personal information.

Electronic identity (eID) is created when a cybernetic identity is paired with a description of a person. The complete electronic identity is stored and protected solely on AIM.

Personal information is any information by which a physical identify can be identified, such as name, contact address, identification card number and biometric data.

2.5. Creating identity and related terms

Identity proofing is a process where a physical identity is paired with a cybernetic-identity. Once the process is complete, the cybernetic-identity allows to use the information about the physical identity that was verified and linked to the cybernetic identity during identity proofing.

Pairing key is a random unique string generated by the administrator and passed on to the user. It must be generated while a new user is being created or verified according to the Pairing Key Scenario. The key is used as a unique identification of a cybernetic-identity when a new user is created. The pairing key must be provided to the user in a secure way. It can also be used when a user loses or forgets their PEIG® and registers a new one in the system.

Registration form ID is a unique identification number that is generated when a new user is being created, according to the Registration Form Scenario. It is used for identity proofing when the user's cybernetic identity is paired with their physical identity in the system.

3. Logging in for the first time via ADUCID®

For application authentication via ADUCID®, a unique cybernetic identity is created for the user during their first authentication to a new provider. This identity is also used for future authentication.

The process is automated. During the first log in, the user only confirms that their identity was created.

The provider may also request registration of their authentication data. The registration process may consist of the following steps:

1. Registration of user's personal data (optional)
2. Verification that the user is the owner of a particular PEIG® and that the personal data are correct (optional)

Registration of a user's personal data is optional and the main goal is to give the provider correct information about the identity of a particular user.

The verification process ensures that:

- The person has the correct identity.
- The person is registered in the system with the correct identity and that the system identifies the person by the correct personal data.

3.1. Creating your identity

Your new identity will be created the first time you log in to a new provider. The procedure is similar for both PEIG-PC (or USB) and for mobile PEIG®.

Proceed as follows:

1. Start your PEIG®.
2. Activate your PEIG®.
3. Start your web browser and enter the address of your identity provider.
4. If this is, indeed, your first connection to a new provider, confirm by clicking **OK**. In case, the current security profile has direct init set, dialog on the picture below will not appear.

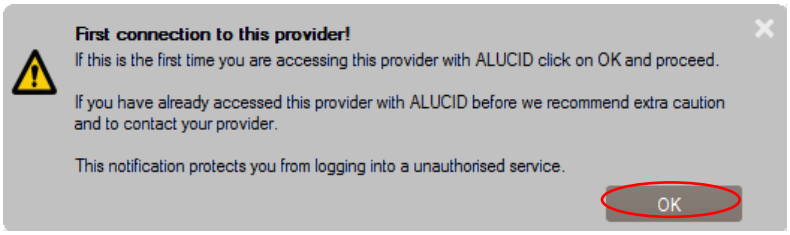


Figure 3-1 Warning about an unknown/new provider

5. Click **Create new identity**. In case, the current security profile has direct init set, page on the picture below will not appear and identity will be initialized automatically.

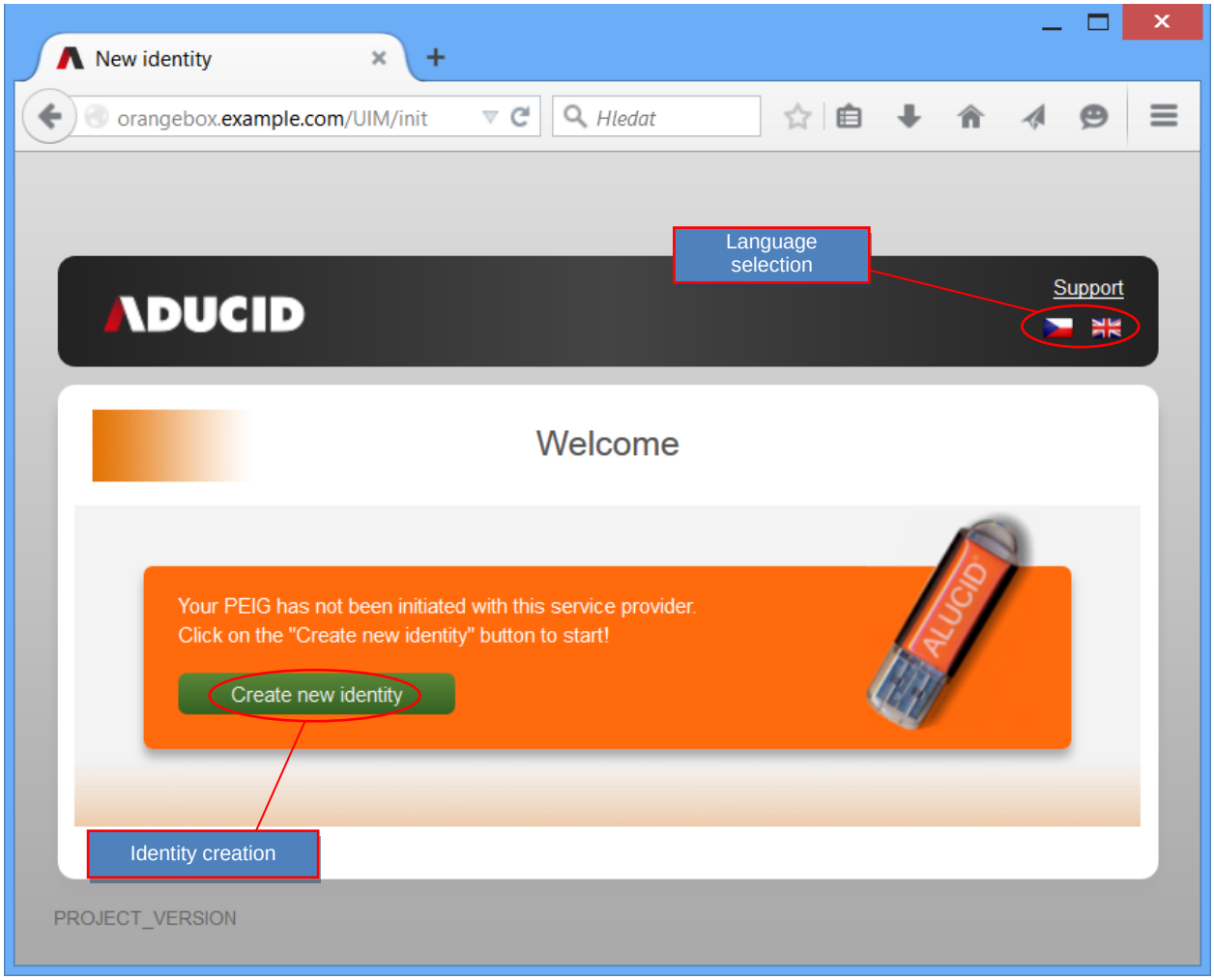


Figure 3-2 New identity creation

6. AIM identification on PEIG®.

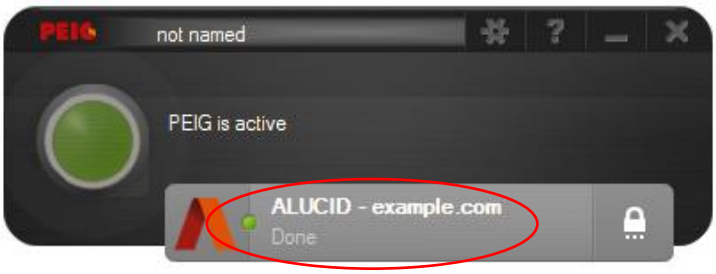


Figure 3-3 PEIG® connected to new provider

7. Now you are forwarded to the intro page of a self-service portal.

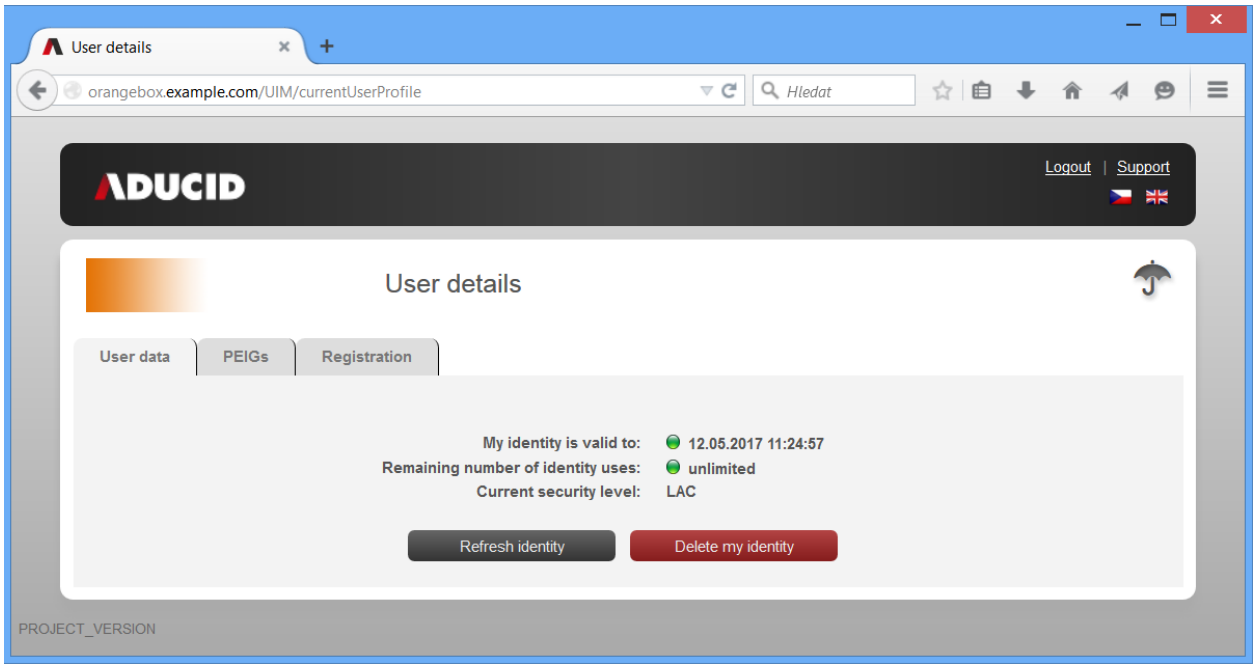


Figure 3-4 UIM – self-service portal for users

3.2. Available registration methods

If you have an identity for a particular provider but your personal data has not been registered or verified, you can usually use at least one of the following registration procedures:

1. Pairing key
2. Registration form
3. Transferring your registration from another provider

ADUCID® also supports a pseudonym mode, which means that you do not have to go through registration and verification at all. The system keeps no personal data about you, and yet ADUCID® is still able to identify a particular user. This mode is especially good in situations when gathering data about users is undesirable for security or economic reasons.

Note:

The following registration procedure assumes that your identity has already been created and that you are connected to UIM.

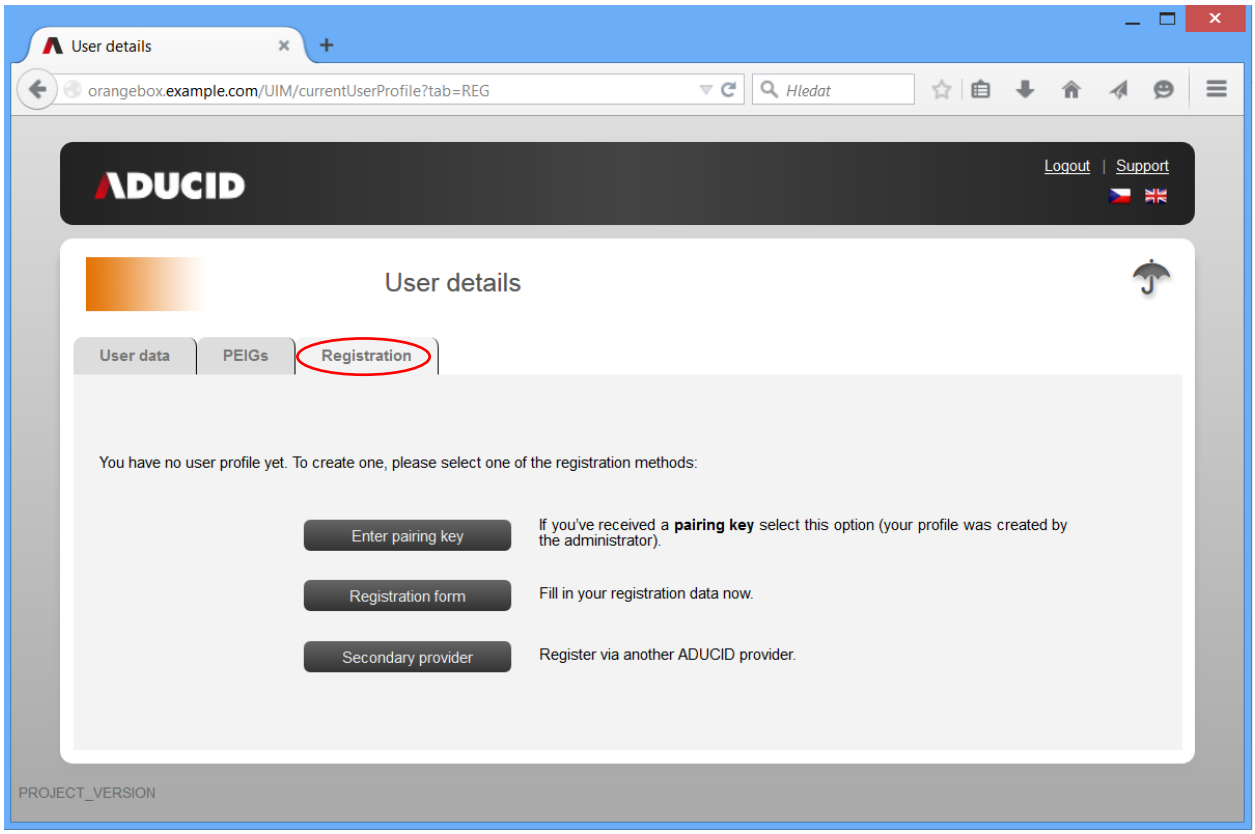


Figure 3-5 Available registration methods

3.2.1. Pairing key registration

The User Manager will provide a pairing key to you and you will use this pairing key when you log in for the first time.

Procedure (for users):

1. In the self-service portal, click **Registration** and select **Enter pairing key**.

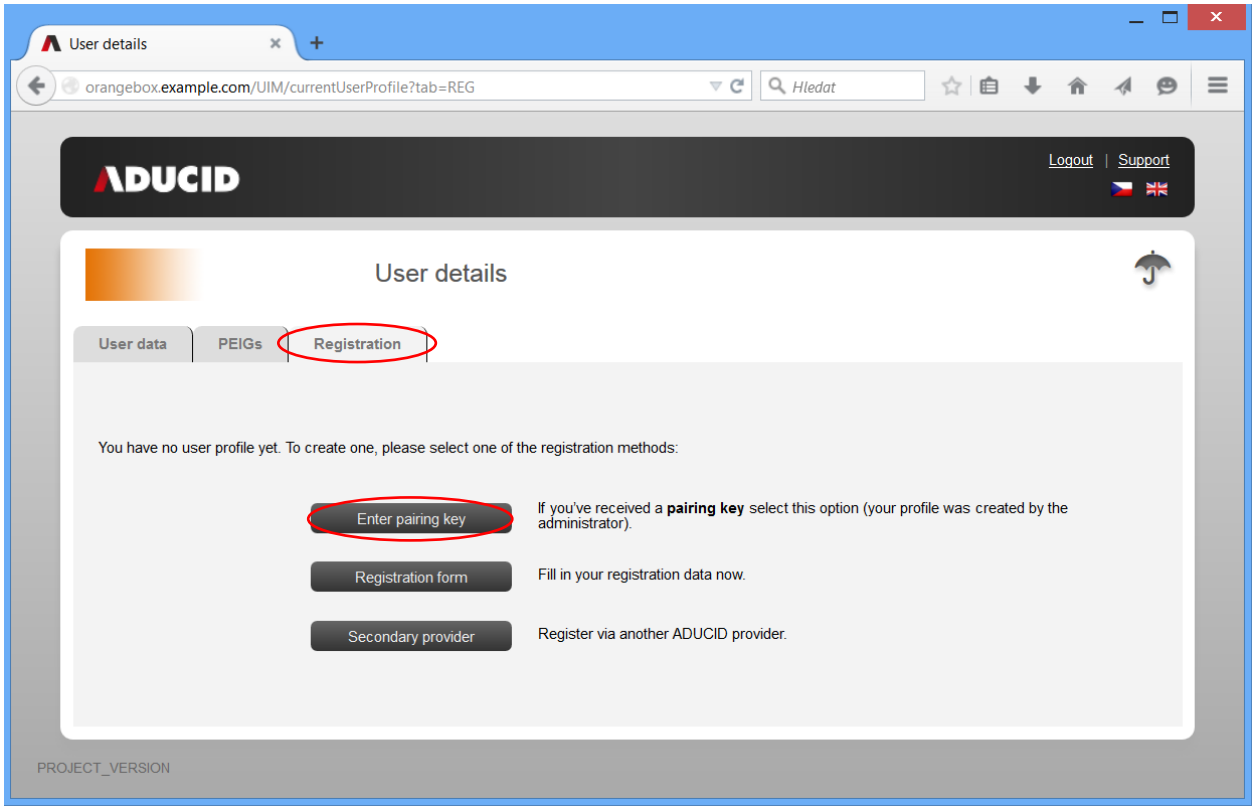


Figure 3-6 Pairing key registration

2. Enter the pairing key that. Click **Confirm**.

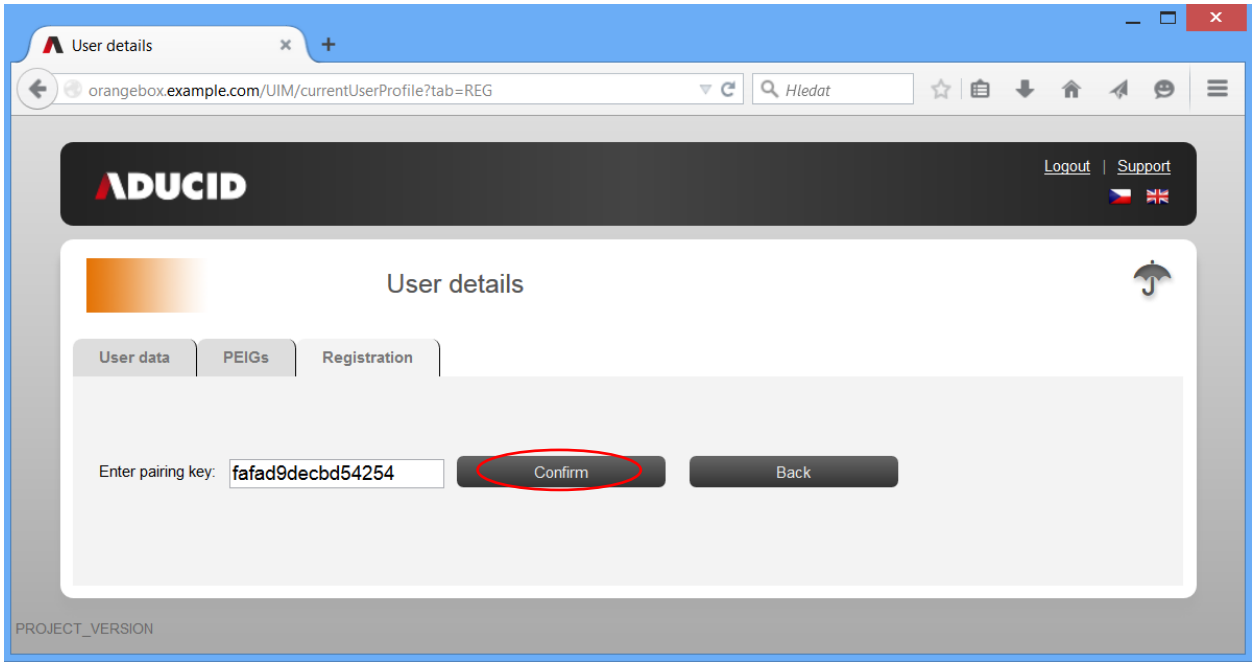


Figure 3-7 Enter your pairing key

3. If the data displayed are correct, click **Data are correct**. If not, click **Data are incorrect**.

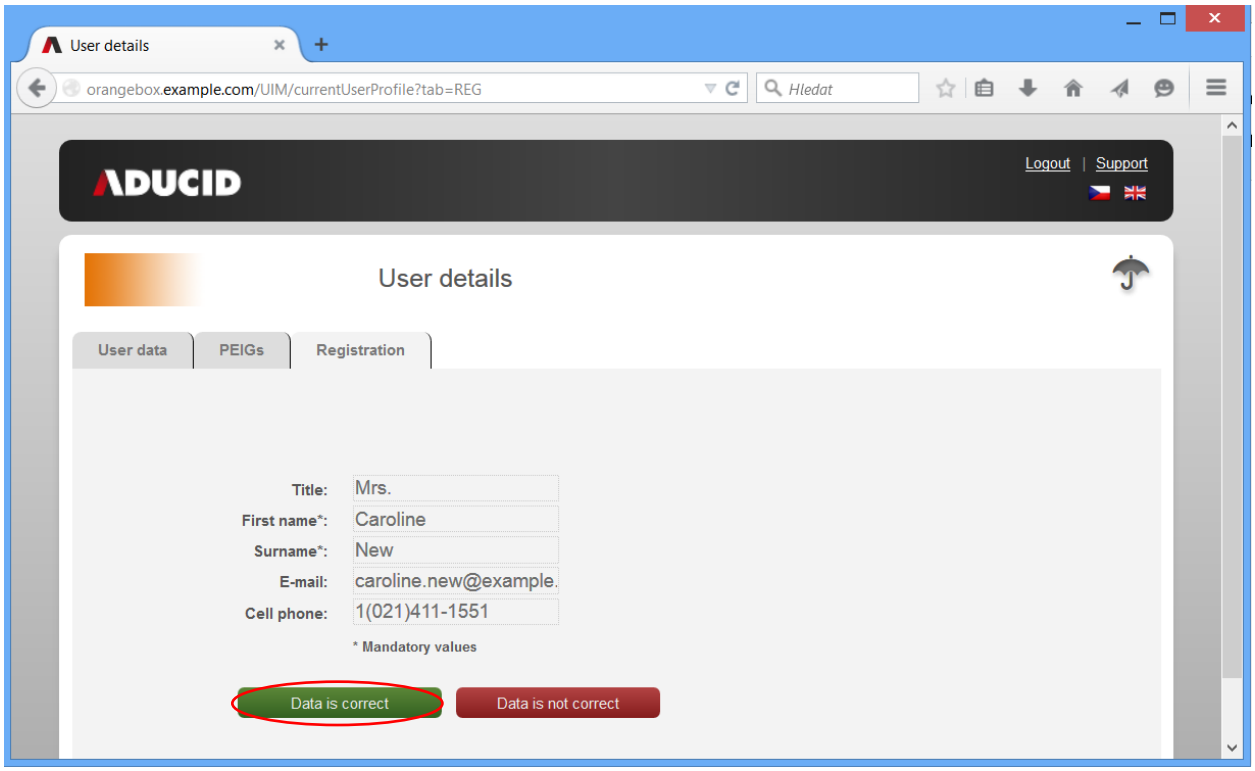


Figure 3-8 Verify and confirm your personal data

4. Once you confirm that the data are correct, you will be informed that the operation succeeded.

Figure 3-9 Information that your identity was successfully paired

Now your cybernetic identity in your PEIG® is paired with your real data in the system. You can now start with your own activities.

3.2.2. Self-service registration (via the registration form)

In this scenario, users register their personal data by using the registration form. The registration form must be provided to the User Manager.

Here is the self-service registration procedure:

1. In the self-service portal, click the **Registration** tab and then click **Registration form**.

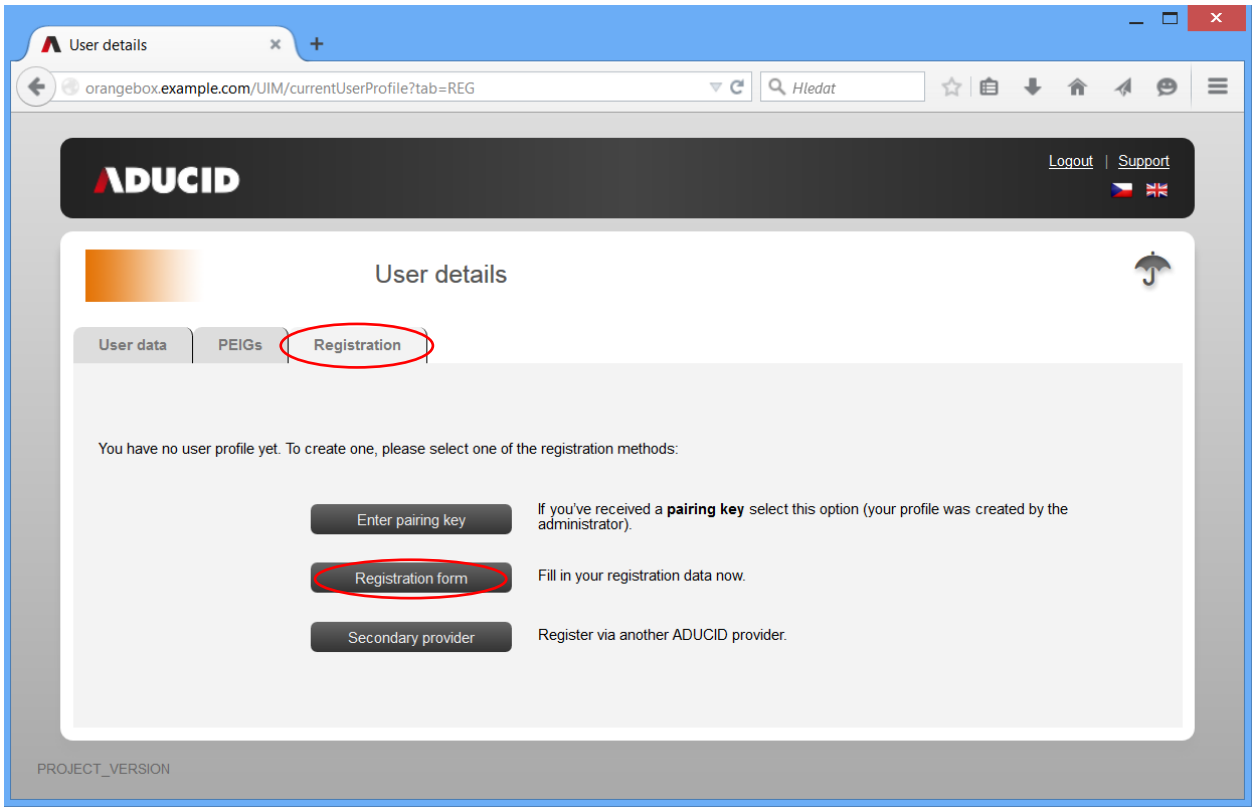


Figure 3-10 Registration via registration form

2. Enter your personal data and click **Create profile**.

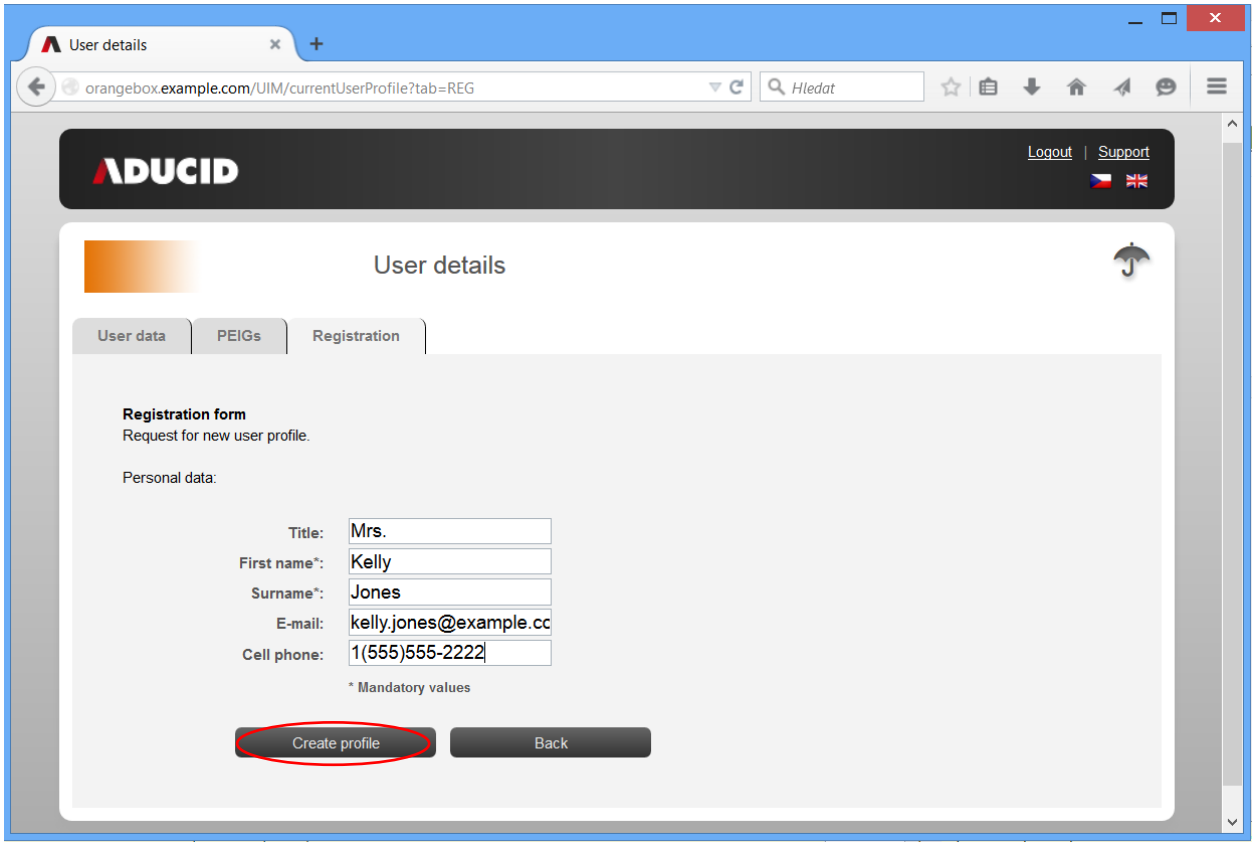


Figure 3-11 Create profile

3. Click **OK**.

Figure 3-12 Notification

4. Print this page, sign it and provide it to the User Manager.

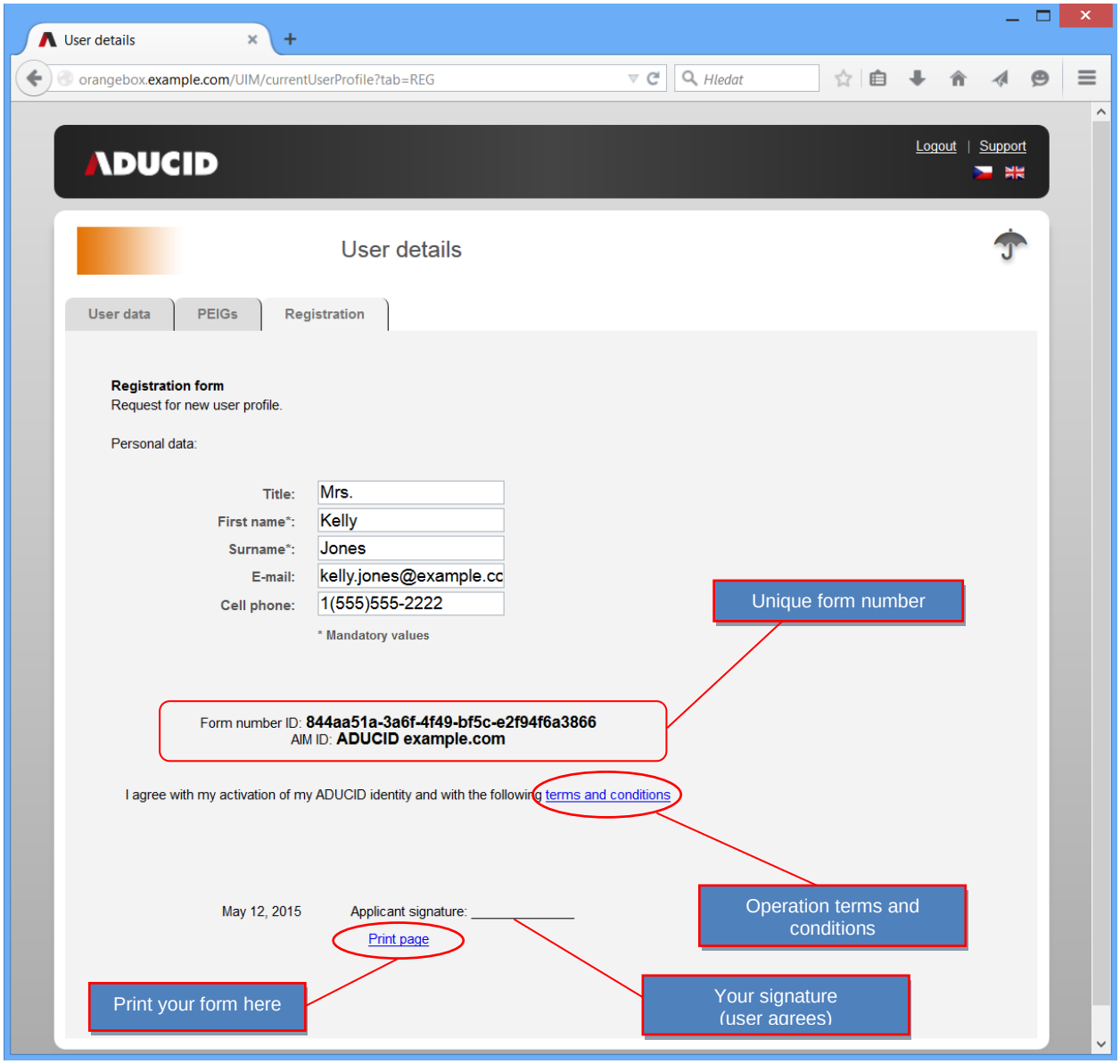


Figure 3-13 Registration form ready to be printed and signed

5. Provide the form or registration number to your provider (if they require it).
6. You are now registered with your new provider.

3.2.3. Transferring an existing registration from another provider

In this scenario, users can transfer their existing, previously verified registration from another provider.

Registration procedure:

1. In the self-service portal, click the **Registration** tab and then click **Secondary provider**.

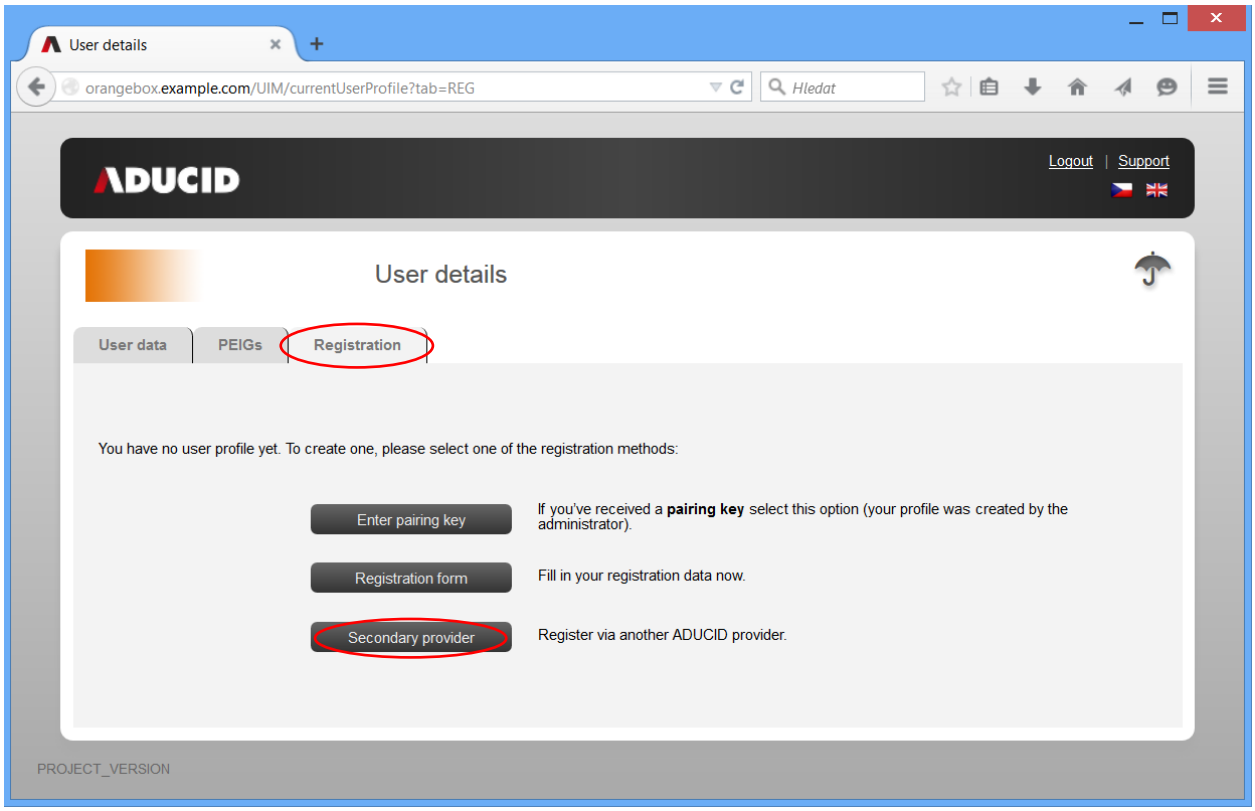


Figure 3-14 Registration transfer

2. Choose the provider with whom you already have an existing account. Your personal data will be transferred from that provider to the current provider. Then, click **Use identity**.

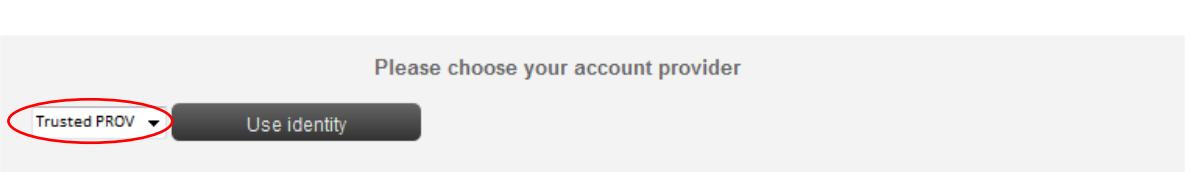


Figure 3-15 Choose your account provider

3. Click **Yes** to confirm the registration transfer.

Figure 3-16 Identity link

4. Personal data management

You can verify and manage your personal data by using the UIM application.

1. Insert your PEIG® into your computer, start it and activate it.
2. Open your web browser and log in to the UIM pages. When managing your identity and personal data, keep in mind that:
   a. Operations with your identity are performed immediately.
   b. Changes of your personal data will not be reflected in the system until the administrator confirms the changes.

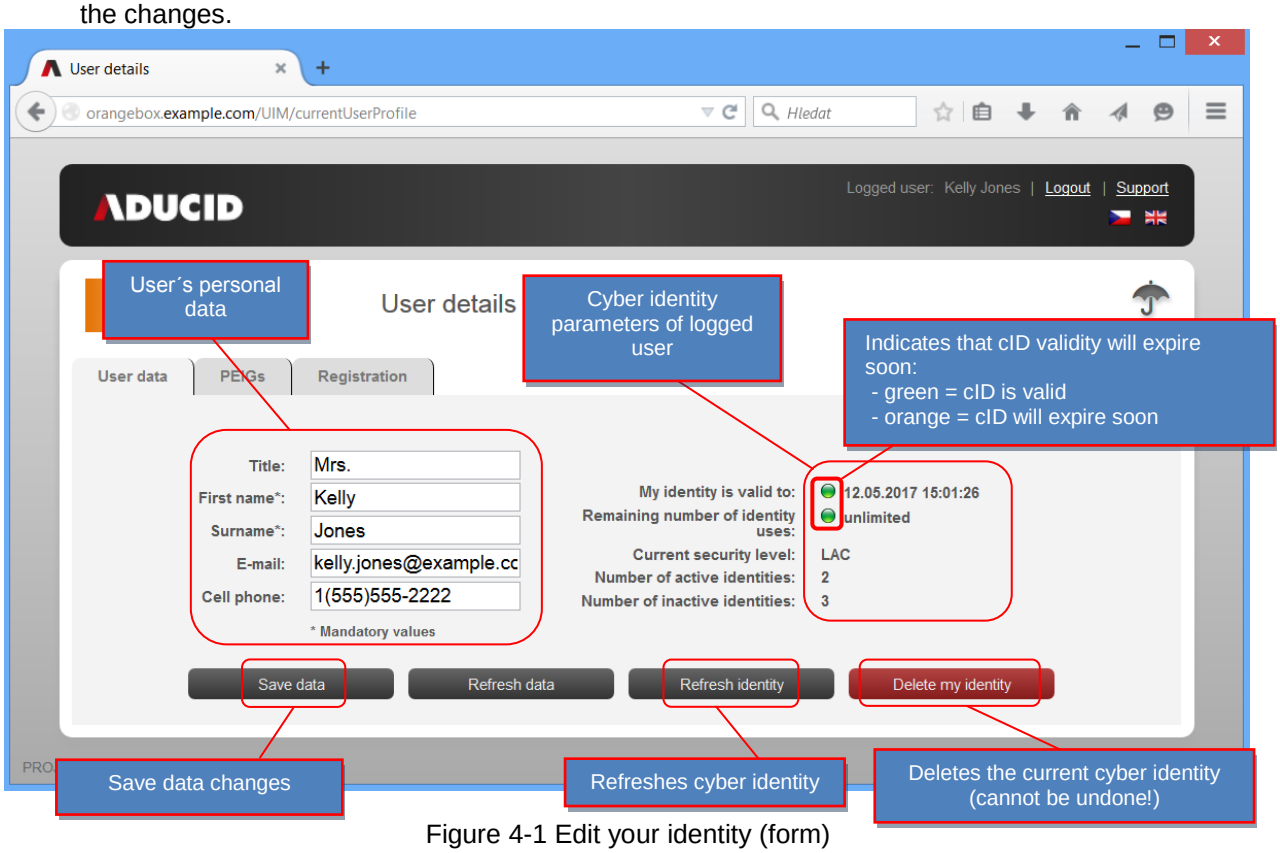


Figure 4-1 Edit your identity (form)

5. User management

The UIM application enables simple and easy management of your identity and PEIGs®, particularly:

- Verify identity and renew its validity
- Delete identity
- Check the number of active and temporarily deactivated identities
- Create a backup identity (replica) for another PEIG®

5.1. Verification of identity validity

Each of your ADUCID® identities is valid for a limited period of time. This validity has two parameters:

1. Validity date and time—how long the identity is valid.
2. Validity count—how many times more an identity can be used. With each operation related to your identity (including authentication), the number decreases by one.

The information about your identity validity can be found on the UIM main page (see Figure 5-1 Edit your identity (form)).

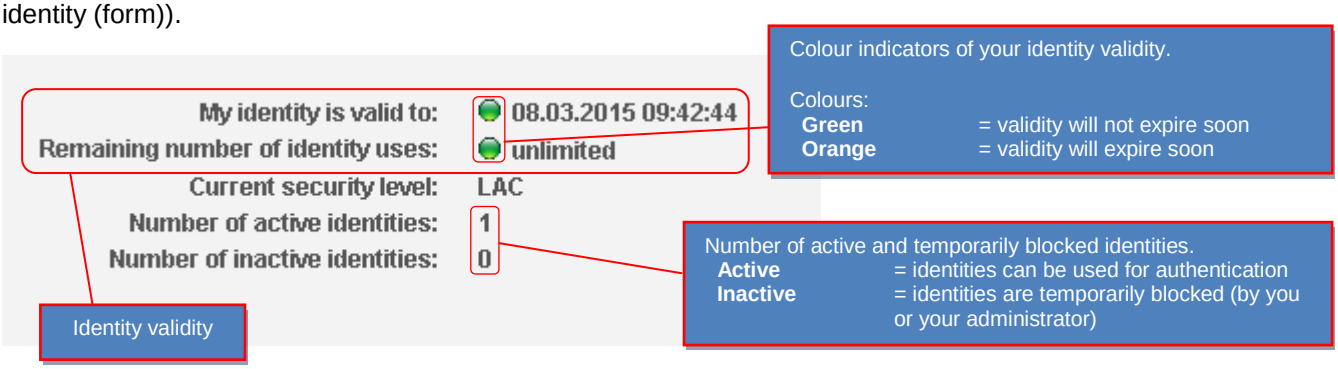


Figure 5-1 Information on identity validity

Once the parameter validity goes below the limit defined by the Security Manager, the green indicator becomes orange (unless an automated identity renewal has been set up).

5.2. Renewing your identity validity

Identity validity renewal is usually an automated process. However, if the security policy of your provider does not allow automated validity renewal, it is necessary to renew the validity manually.

The validity can be renewed by **Generate new identity**.

When do you have to renew your identity manually?

1. If you do not have a PEIG® with hardware protection and you suspect that your identity protection has been compromised (e.g. you left your PEIG® unattended at a public place), always perform this operation in a secure environment. By changing your identity, you will cut the attacker off (supposing that you perform this operation in a secure zone and the attacker does not have access to your PEIG® any longer).
2. If the green indicator becomes orange, your identity validity will expire soon.

Click **Generate new identity**. Your new identity with new parameters will be generated (Including a new validity period and new cryptographic secrets), and it will replace your previous identity.

If the remaining number of your identity uses equals zero, renew your identity immediately or you will no longer be able to log in with this identity. If the identity validity expires, the user is not permitted to log in to any application (including UIM), as an expired identity can never be used for authentication.

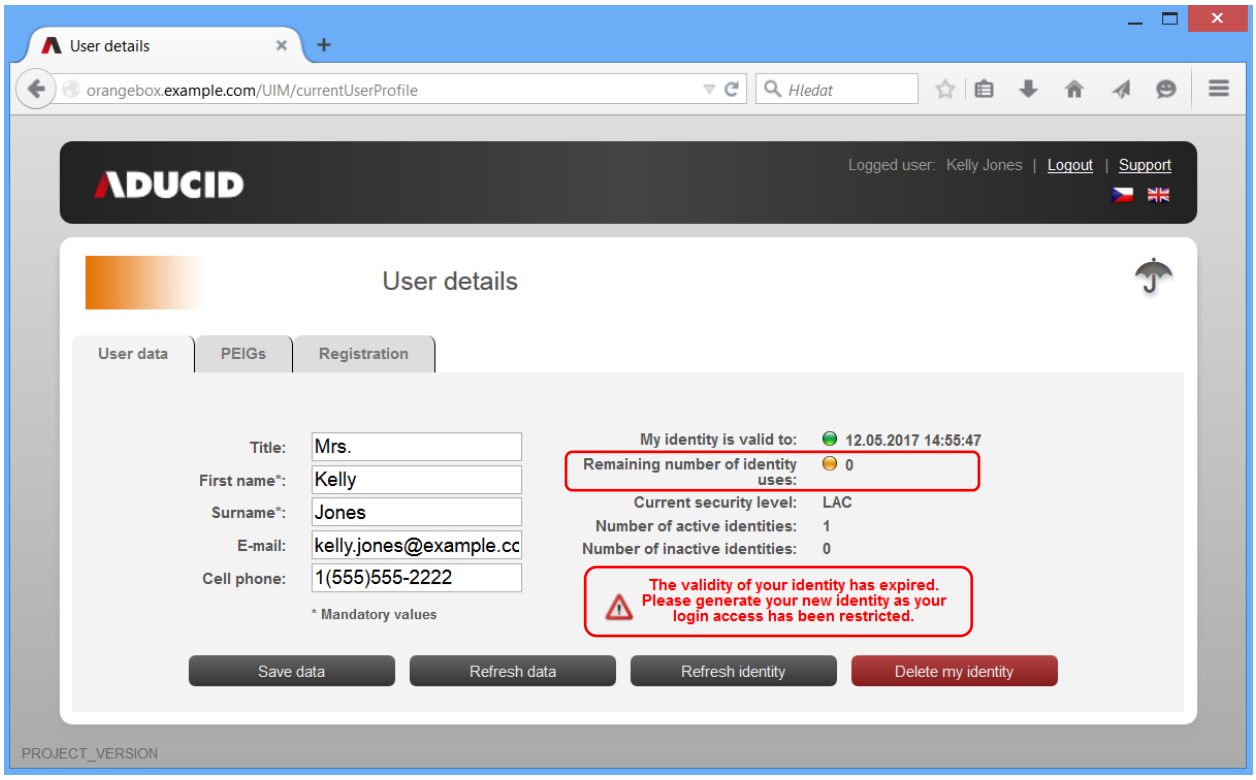


Figure 5-2 Immediately renew your identity

5.3. Deleting your identity

If you want to remove your identity , click **Delete my identity**. Click **OK,** to confirm that you wish to delete your identity.

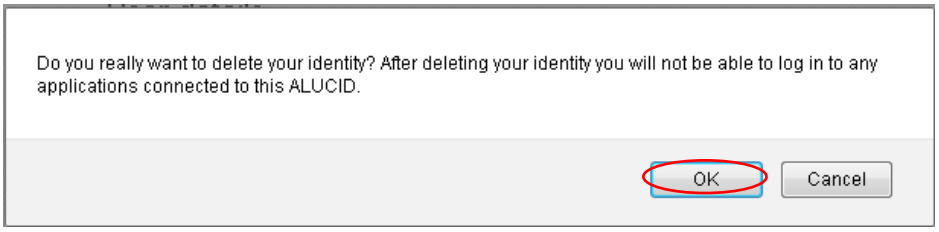


Figure 5-3 Confirm identity deletion

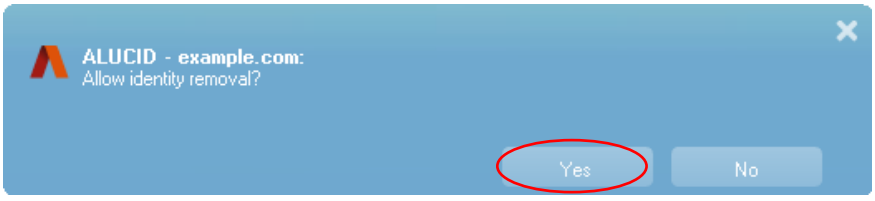


Figure 5-4 Allow identity removal

5.4. Creating your identity replica to backup PEIG®

Losing your PEIG® means losing your user access rights. ADUCID® enables you to replicate your identities to backup PEIGs. If your original PEIG® is lost or there is a malfunction, you can still use your PEIG® with a backup identity.

During replication process you will be asked to confirm some dialogs on original/backup PEIG®:

- Confirm picture icons, where confirmation button will appear in the dialog on the original PEIG®

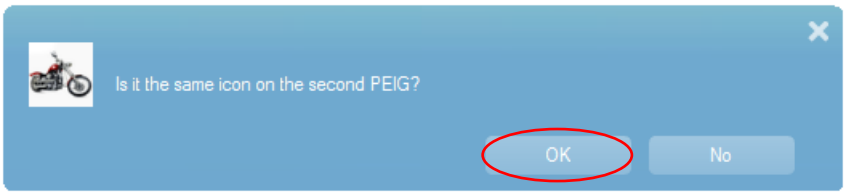


Figure 5-5 Dialog on the original PEIG®

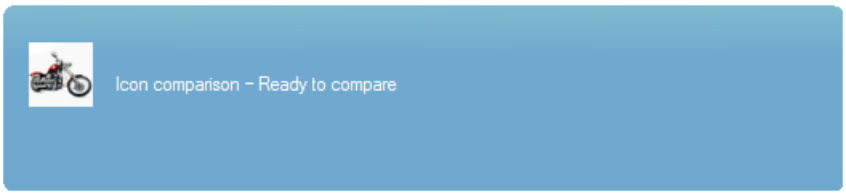


Figure 5-6 Dialog on the backup PEIG®

- Personal factor verification, if it exists on the original PEIG®

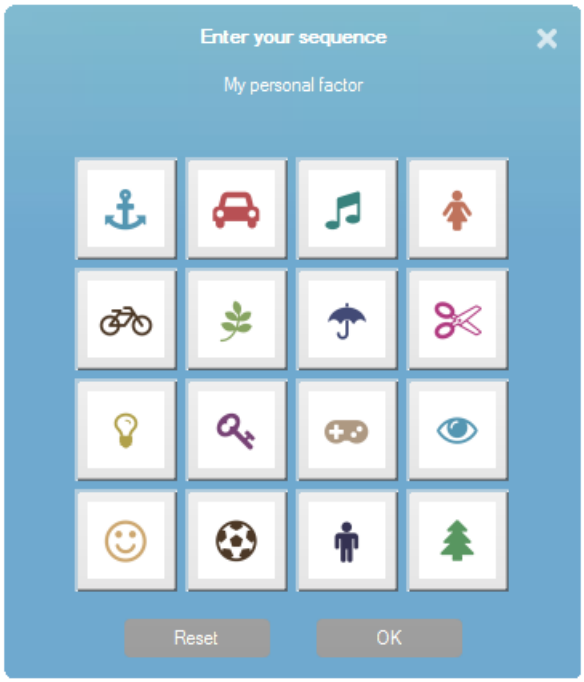


Figure 5-7 Personal factor verification

Backups can be realized on the “PEIGs” page. Backup scenarios are described in the chapters below.

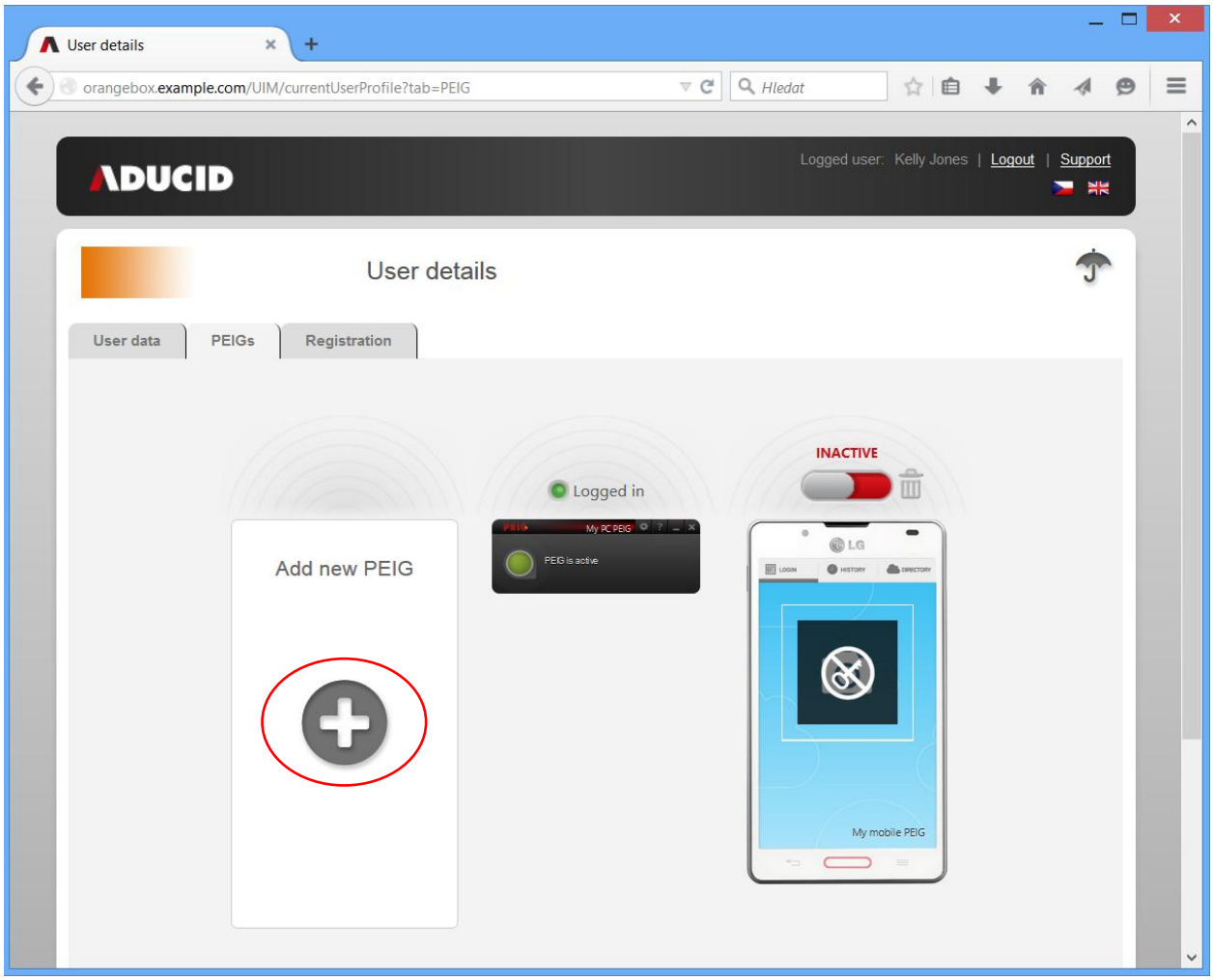
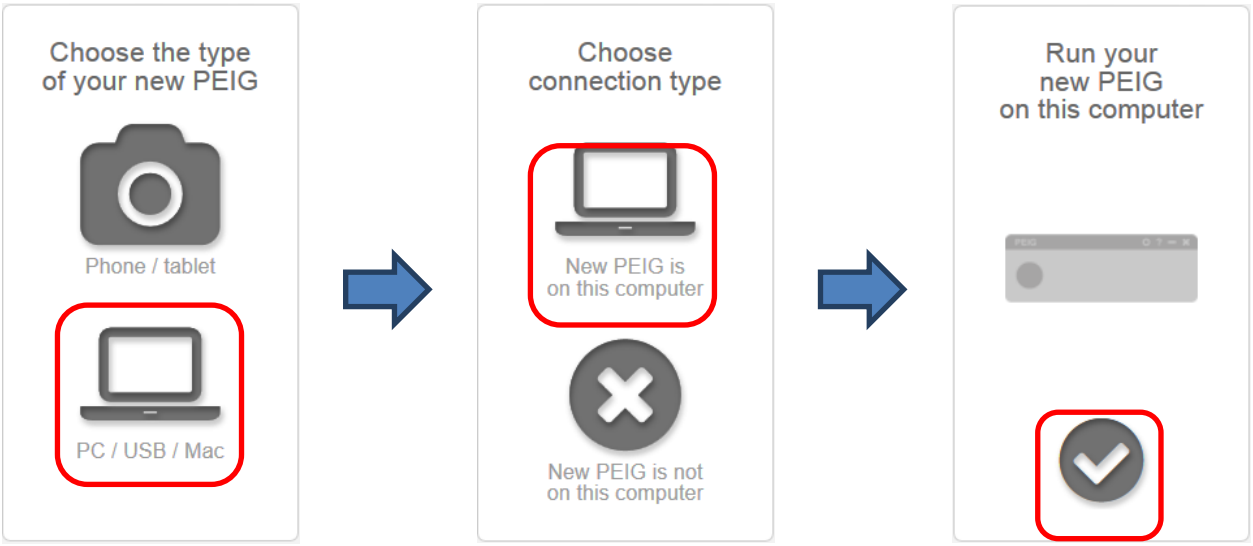


Figure 5-8 Adding new PEIG®

5.4.1. Replica from mobile PEIG® to PC-PEIG®/USB-PEIG®

It assumes, you are logged in to UIM by your mobile PEIG® on desktop. During replication process you will take a QR code photo by the original mobile PEIG®.

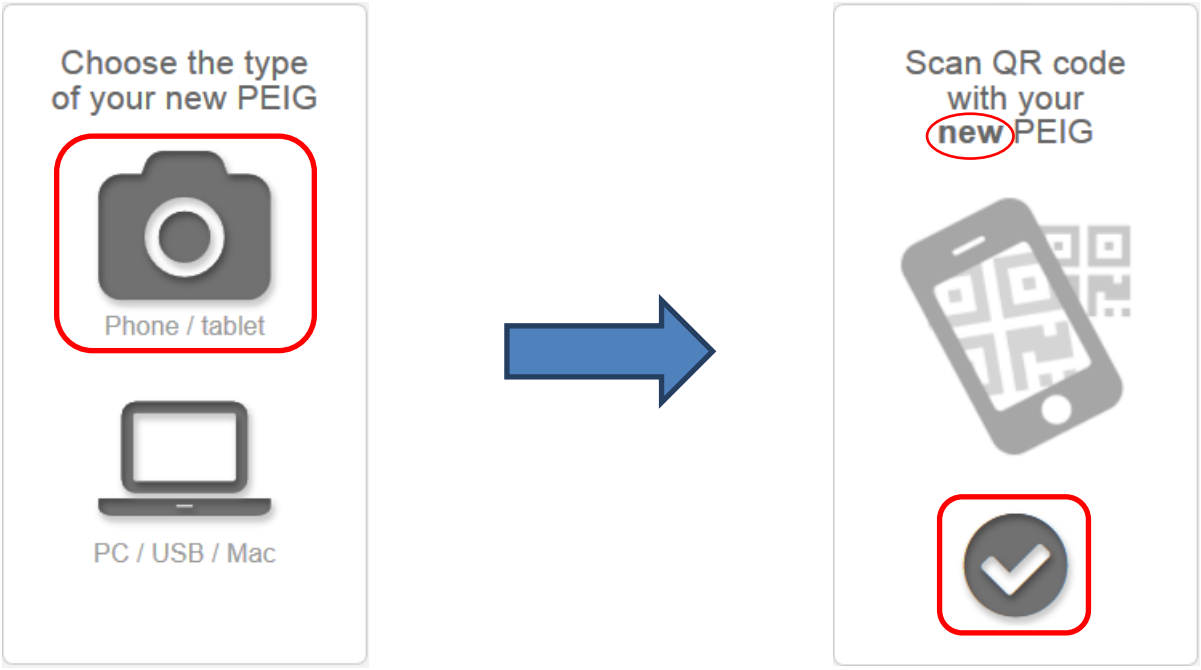
- Start web browser on PC and go on to the UIM page. **Your PC-PEIG®/USB-PEIG® must be switched off in this moment.**
- Log in to UIM by taking QR code photo with mobile PEIG® (Android-PEIG®, or iPhone-PEIG®).
- **Switch on PC-PEIG®/USB-PEIG®.**
- Click on the „+“ picture to start replication and then follow the instructions below.



5.4.2. Replica from PC-PEIG®/USB-PEIG® to mobile PEIG®

It assumes, you are logged in to UIM by your PC-PEIG®/USB-PEIG®. During replication process you will take a QR code photo by the backup mobile PEIG®.

- Start web browser on PC and go on to the UIM page. **Your PC-PEIG®/USB-PEIG® must be switched on in this moment.**
- Logging in to UIM will process automatically, it is not necessary to take a QR code photo.
- Click on the „+“ picture to start replication and then follow the instructions below.

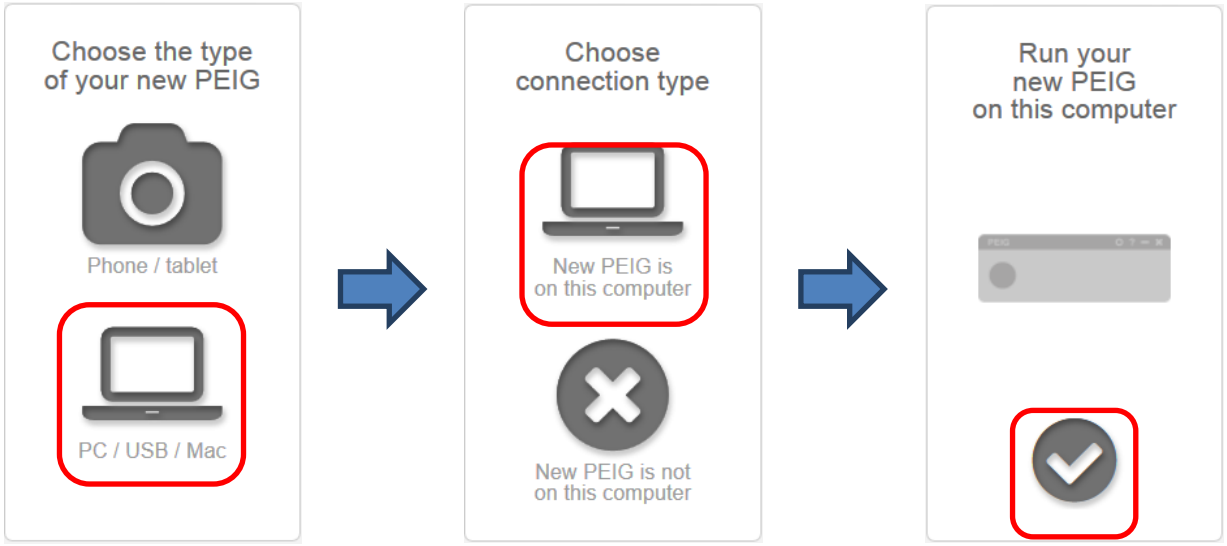


5.4.3. Replica from PC-PEIG® to USB-PEIG®

It assumes, you are logged in to UIM by your PC-PEIG®.

- Start web browser on PC and go on to the UIM page. **Your PC-PEIG® must be switched on in this moment.**
- Logging in to UIM will process automatically, it is not necessary to take a QR code photo.

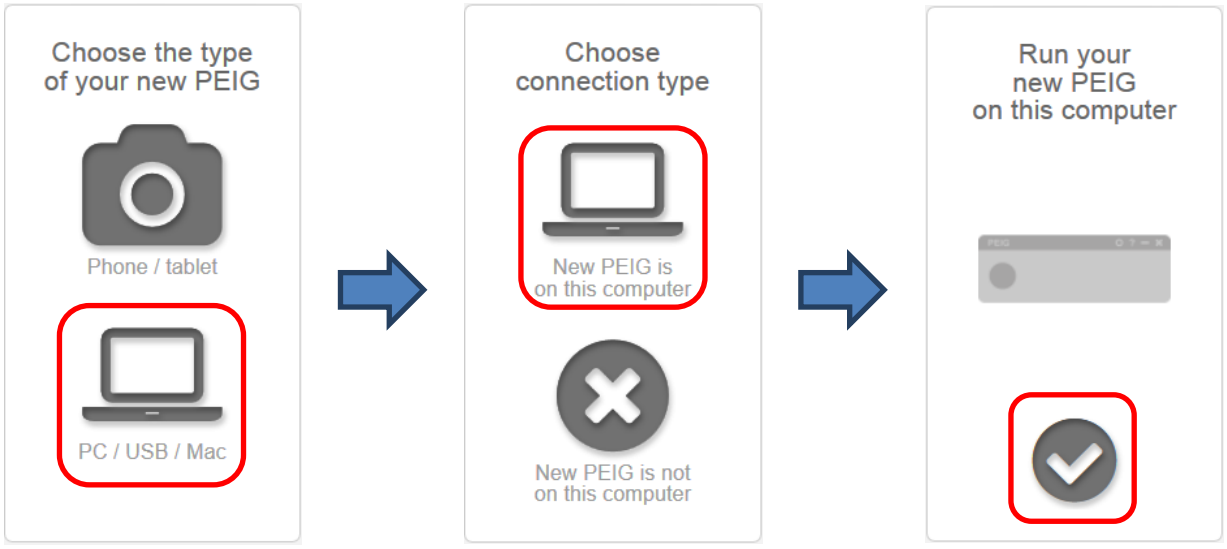
- **Connect USB-PEIG® to the computer and verify, it is switched on**.
- Click on the „+“ picture to start replication and then follow the instructions below.



5.4.4. Replica from USB-PEIG® to PC-PEIG®

It assumes, you are logged in to UIM by your USB-PEIG®.

- Start web browser on PC and go on to the UIM page. **Your USB-PEIG® must be switched on in this moment.**
- Logging in to UIM will process automatically, it is not necessary to take a QR code photo.
- **Switch on PC-PEIG®**.
- Click on the „+“ picture to start replication and then follow the instructions below.



5.4.5. Replica from mobile PEIG® to mobile PEIG®

It assumes, you are logged in to UIM by your mobile PEIG® on desktop. During replication process you will take a QR code photo by the original mobile PEIG® than by the backup PEIG®.

- Start web browser on PC and go on to the UIM page. **Your PC-PEIG®/USB-PEIG® must be switched off in this moment.**
- Log in to UIM by taking QR code photo with mobile PEIG® (Android-PEIG®, or iPhone-PEIG®).

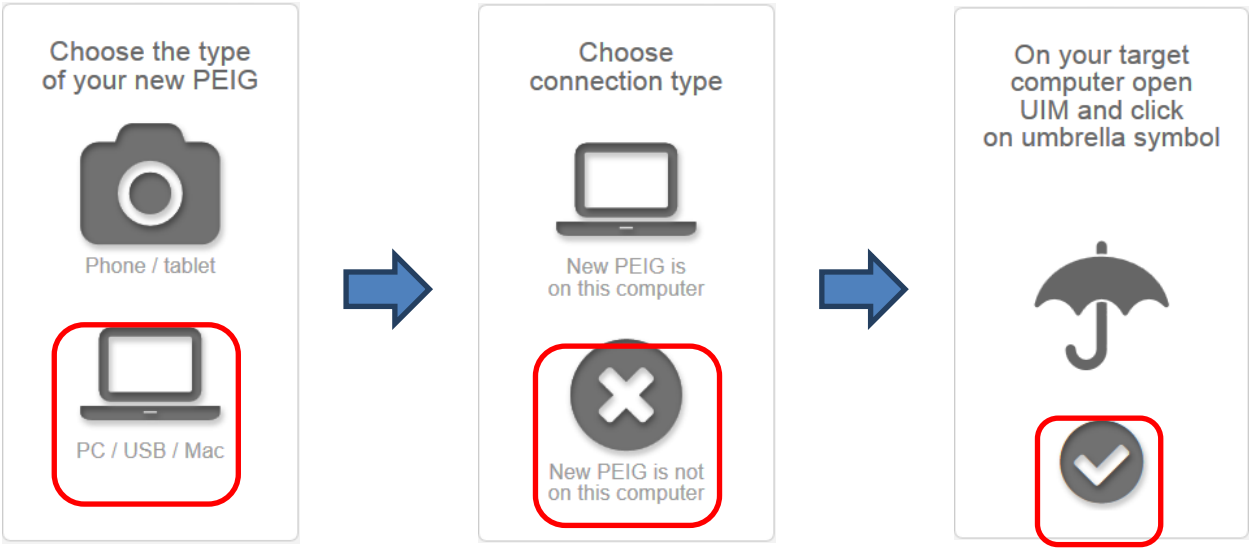
- Click on the „+“ picture to start replication and then follow the instructions below.

5.4.6. Replica over “Meeting room” – without dependency on the PEIG® type

It exists way, how to realize PEIG® replication without dependency on the PEIG® type. This scenario assumes, that both original and backup PEIG® have access to UIM application and PEIGs are not running on the same device. Chapters below describe, which steps are necessary to realize, at first with the original PEIG® than with backup PEIG®.

5.4.6.1. Original PEIG® preparation

At first we start backup page where we can add new PEIG® and then realize steps below.



Than picture keyboard will appear. There we choose unique picture sequence, which we must remember to be used during backup PEIG® preparation.

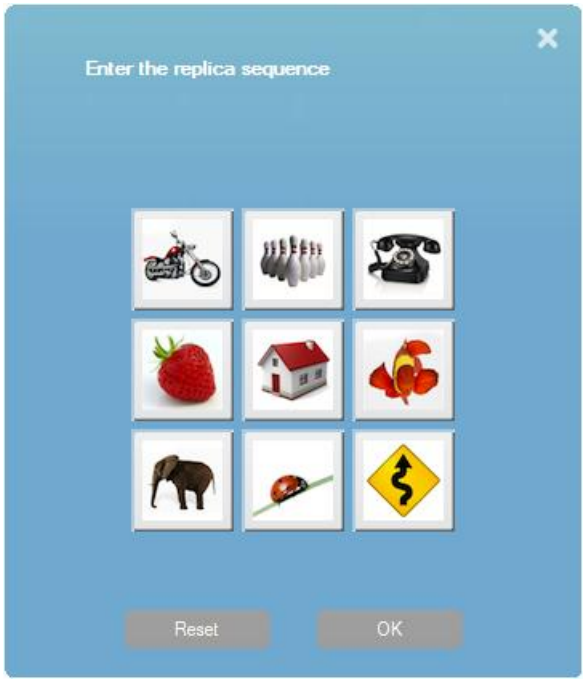


Figure 5-9 Picture keyboard for replica

Now original PEIG® is ready to be replicated and it is waiting for backup PEIG® preparation steps.

5.4.6.2. Backup PEIG® preparation

Now we access application with backup PEIG® and click on the umbrella picture, which can be found on the right top corner on the user profile page.

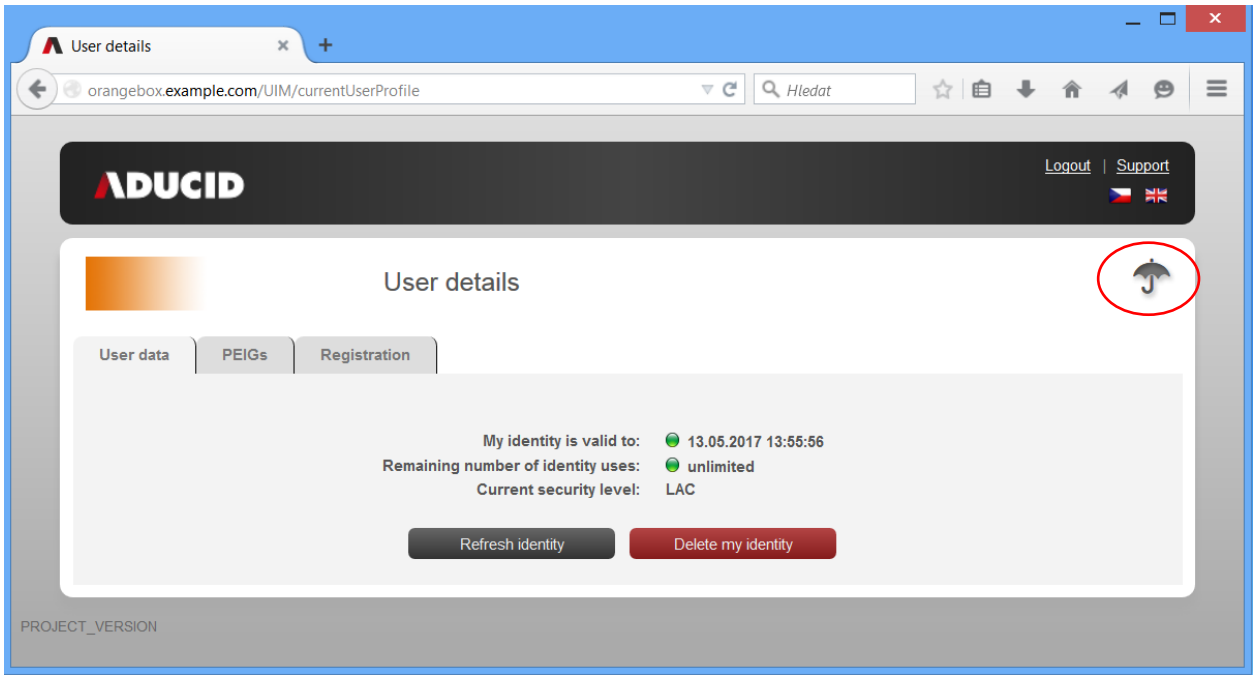


Figure 5-10 Umbrella picture

Now we will see picture keyboard where we choose picture sequence which we choose during original PEIG® preparation. In case of right picture sequence, user will be asked to confirm icons appeared on the both PEIGs, or to verify personal factor, if necessary. If all these steps are successfully finished, replica is done.

6. Management of PEIGs®

The list of PEIGs® in your possession can be seen on the **PEIGs** tab. You can block the selected PEIGs® here (for example, when you lose them). If you need to deactivate a PEIG®, switch its status from **Active** to **Inactive**. It is also possible to remove selected PEIG® by clicking on the recycle bin picture. Only inactive PEIG® can be removed.

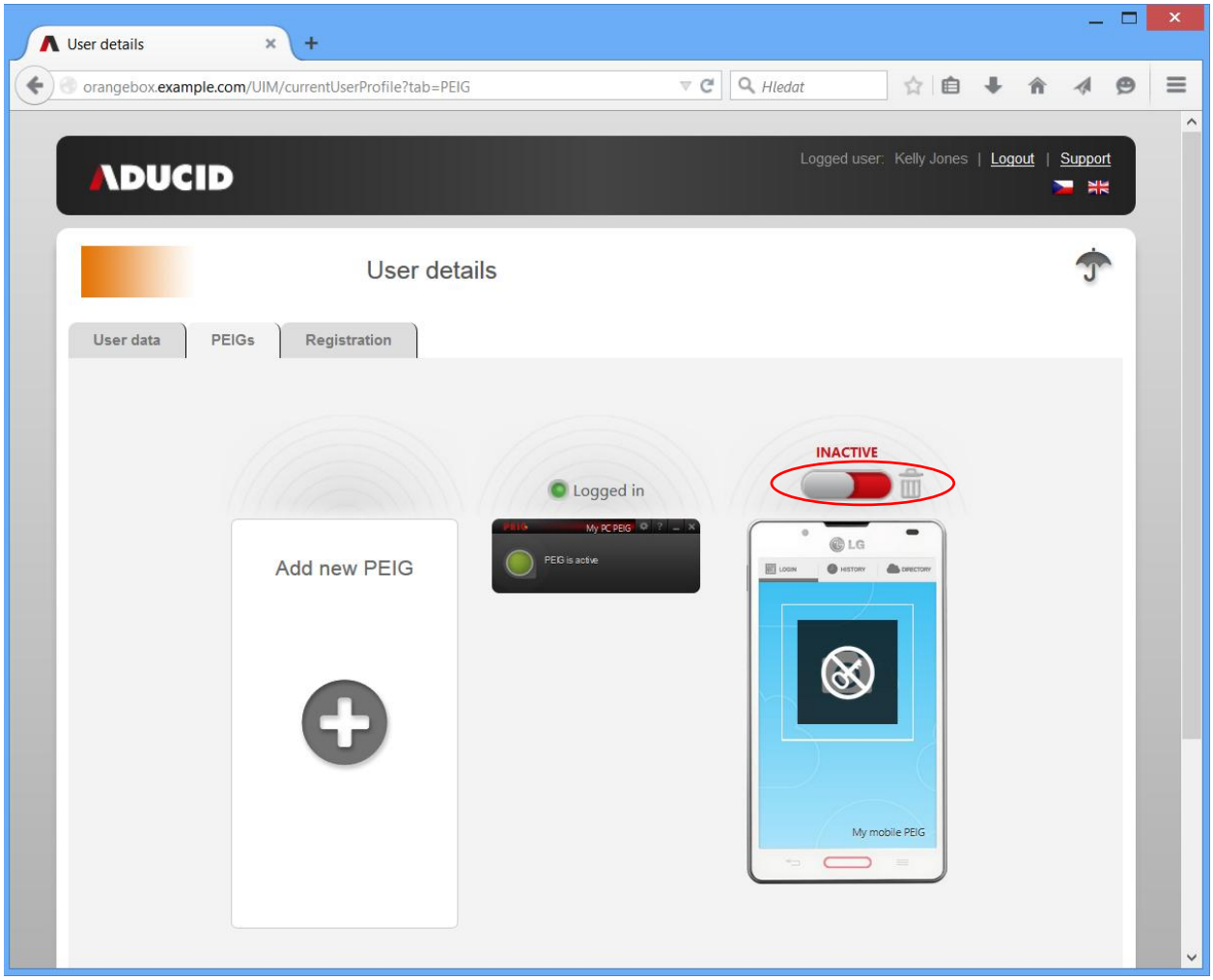


Figure 6-1 List of PEIGs®

In case, current PEIG® has personal factor set, personal factor verification will be required before other PEIG® activation/deactivation/removal operation.

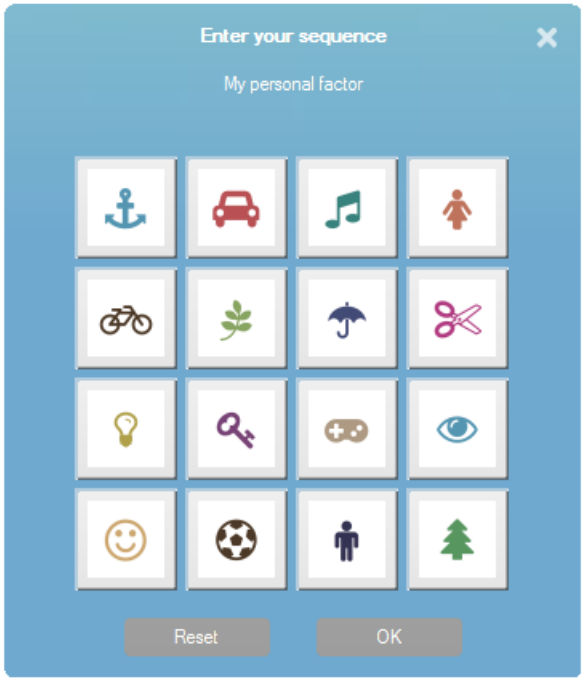


Figure 6-2 Personal factor verification

The PEIG® with which you are currently logged in cannot be deactivated.

7. Common questions and solutions

The following operation or security issues can appear when you access UIM or manage your identities, and you need to react to them. This chapter describes the most important questions about PEIG®.

Action	Error / problem	Possibly caused by
Log in to UIM	System error	Incorrect activation secret
Log in to UIM	PEIG® missing	PEIG® missing or not activated
Log in to UIM	Identity integrity compromised	- Fake AIM - Using expired identity - Using deactivated identity
Log in to UIM	Identity expired	- Fake AIM - Using expired identity - Using deactivated identity

Table 7-1 Most frequent problems

7.1. PEIG® system error

Problem: Unsuccessful log in to UIM. The **System error** message is displayed.

Possibly caused by: An incorrect activation secret may have been entered.

Solution: Make sure that you enter the correct activation secret into PEIG®. If you are sure that you are entering the correct secret, contact the Support team.

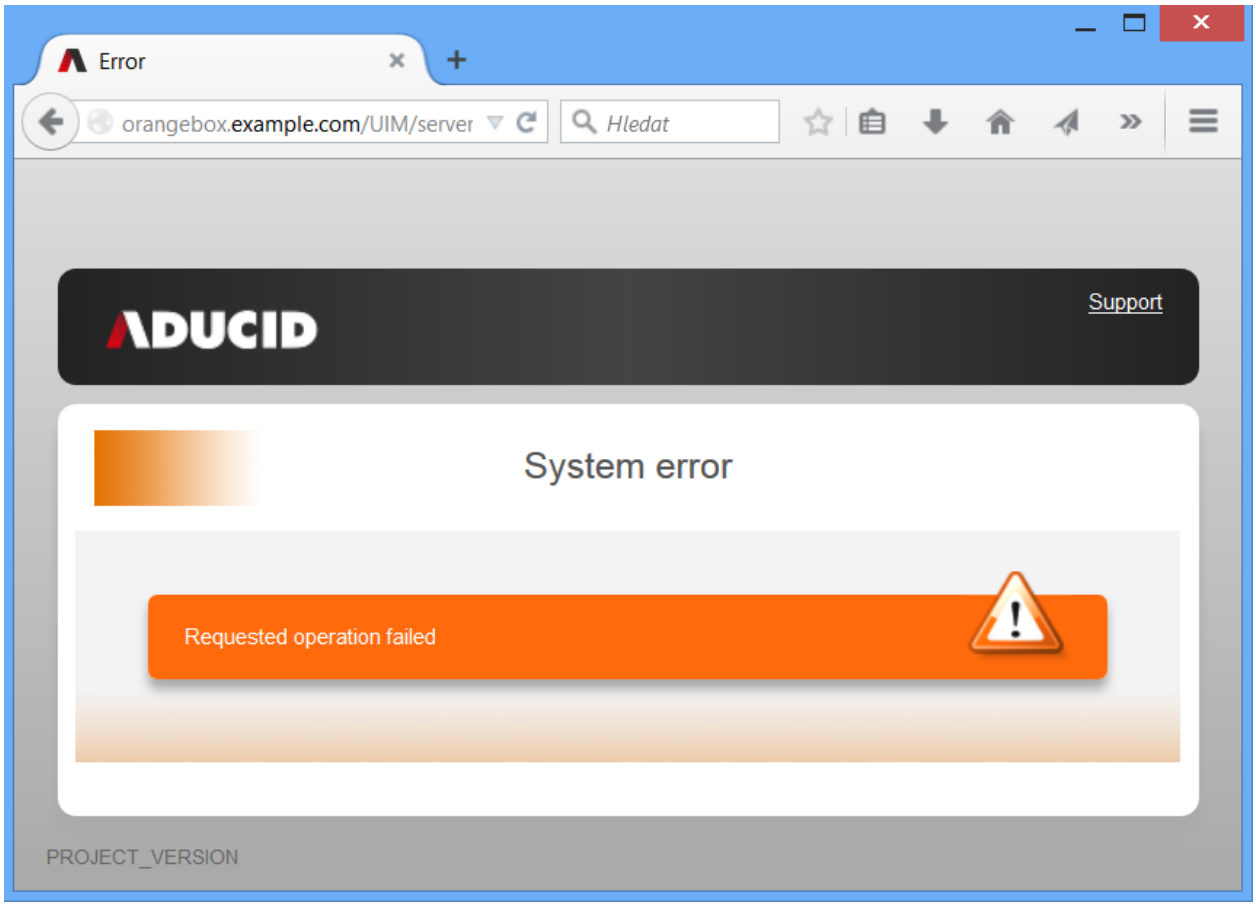


Figure 7-1 System error

7.2. PEIG missing or not activated

Problem: During your log in to UIM, the “PEIG missing / not activated” message is displayed.

Possibly caused by: Your PEIG® is probably not running or it has not been activated.

Solution: Check whether your PEIG® is running and activated—the PEIG indicator must be green and the status must be **PEIG is active**.

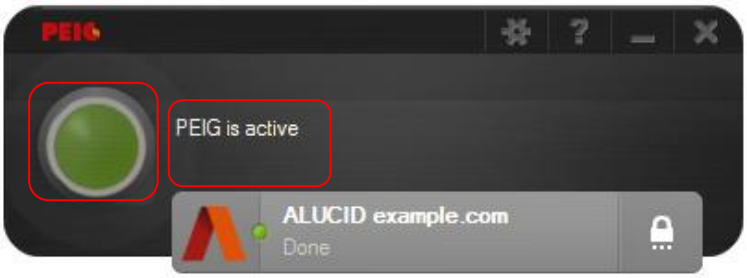


Figure 7-2 Verifying PEIG functionality

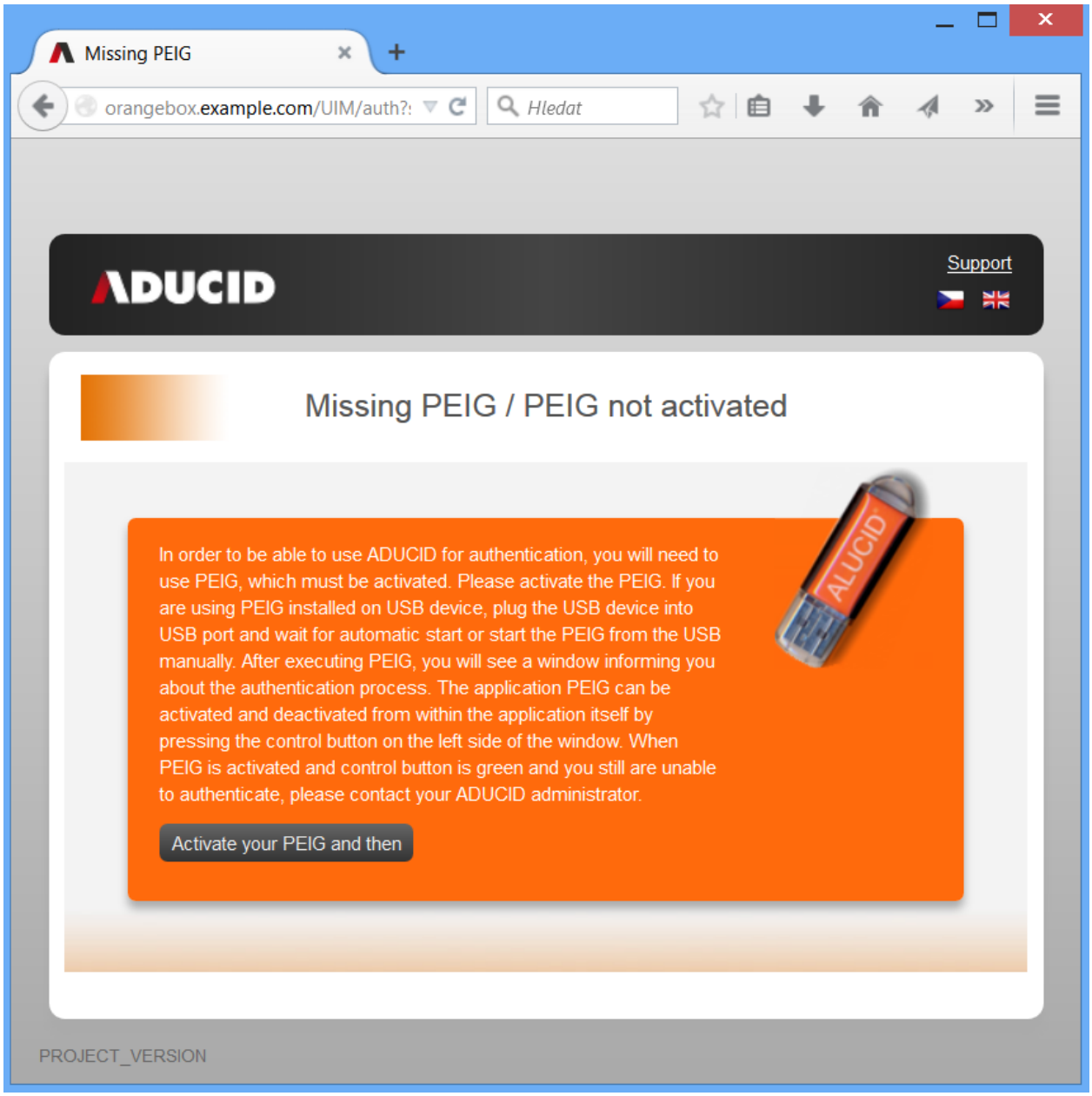


Figure 7-3 Missing PEIG®

7.3. Identity attacked

Problem: Unsuccessful log in to UIM. During your log in to UIM, the following warning is displayed “Identity integrity compromised”. This happens when your identity has not been found in AIM.

Possibly caused by:

- Fake AIM
- Your identity copy has been stolen or it has not been approved
- The AIM provider deleted your identity

The first two situations are serious security incidents. If you are sure that the provider had no reason to delete your identity, inform your AIM provider immediately.

Solution:

1. Check whether you communicate with the correct AIM. If you cannot do that on your own, go to step 2.
2. If the procedure for this situation is described in the operation instructions of your identity / application provider, reinitialize your compromised identity on your own. Otherwise, go to step 3 and do not attempt to reinitialize on your own.
3. Contact your identity or application provider and follow their instructions.

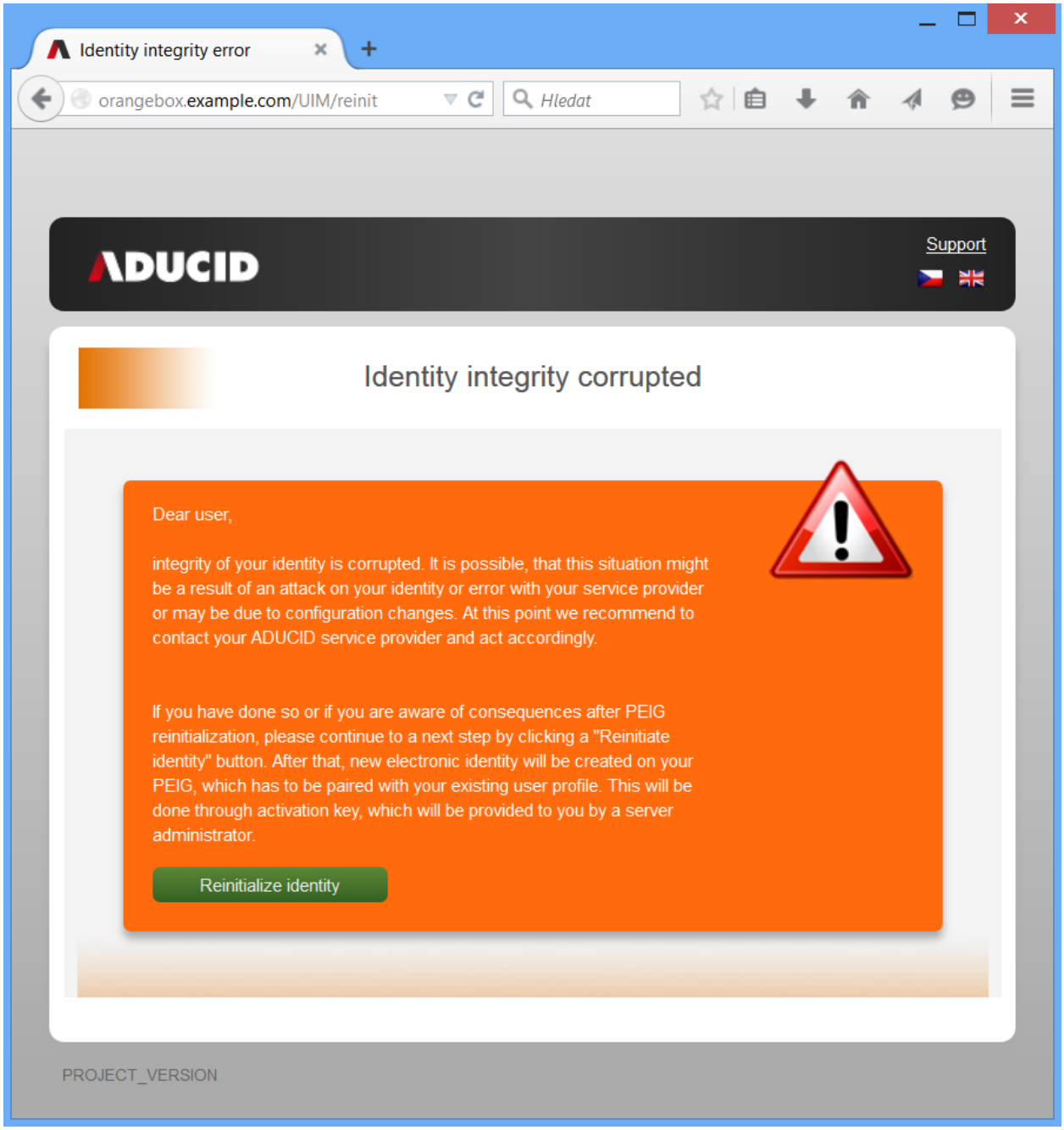


Figure 7-4 Identity integrity compromised

7.4. Identity expired

Problem: Unsuccessful log in to UIM, the “Expired identity” message is displayed.

Possibly caused by: Your identity is expired.

Solution: Renew your identity by clicking **Renew identity**. If your AIM provider is not allowed to renew your expired identity, you need to ask the provider for a new identity.

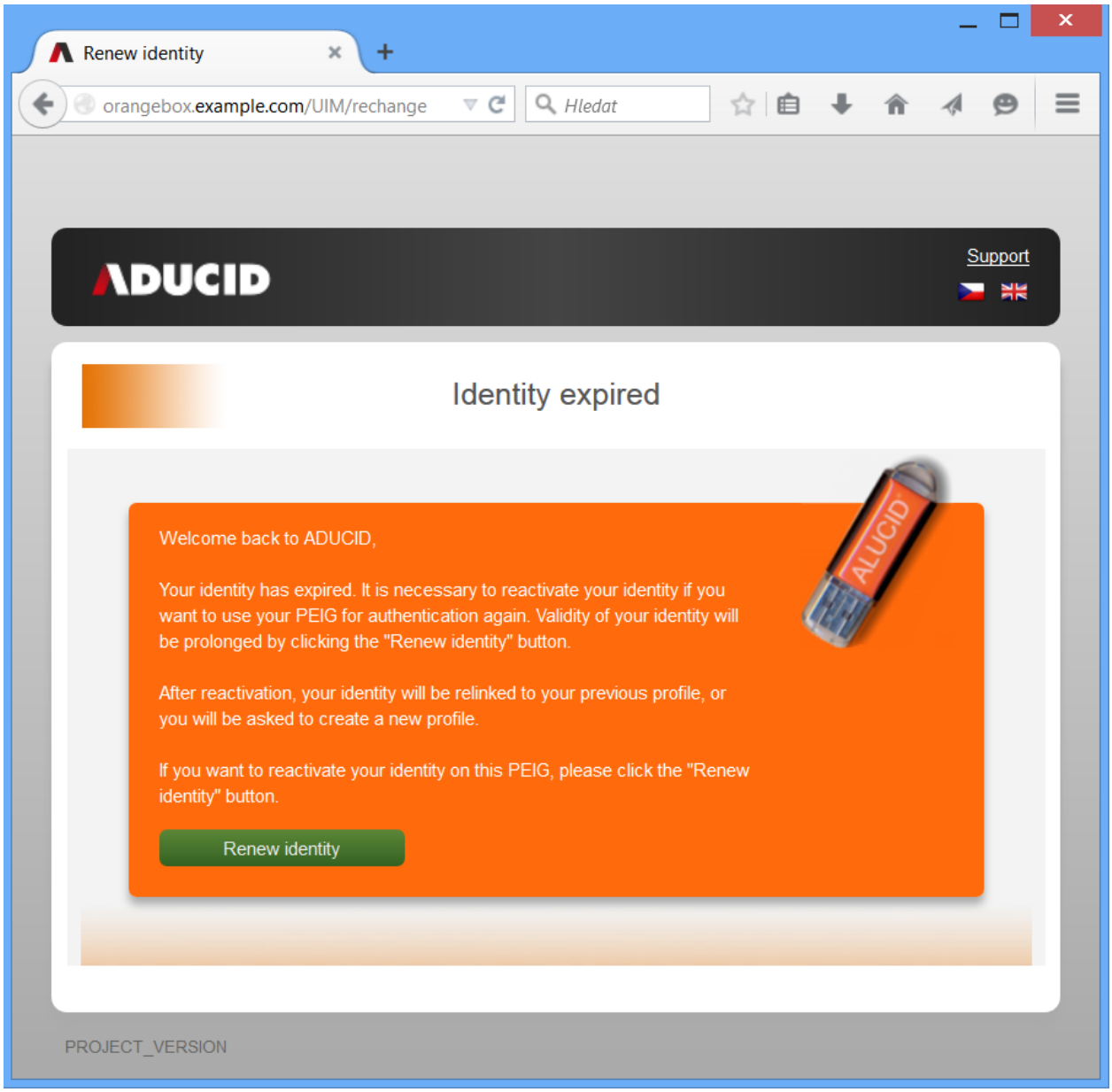


Figure 7-5 Expired identity