ANECT

UIM − Administration 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 administrators of the User Identity Manager (UIM) pro ADUCID® application.

This Administrator Guide includes:

- ADUCID® key terminology
- List of activities and roles in UIM
- First log in and implementation of UIM
- Administrator role management
- User management
- Management of ADUCID® security parameters
- Used licences statistics monitoring

1.2. ADUCID® key terminology

Personal Electronic Identity Guardian (**PEIG®**) is a device that can manage end user's electronic identities. PEIG® also provides automatic authentication between client and server side of a target application.

1.3. What is AIM

ADUCID® Identity Machine (AIM) is software operated by an identity provider. It manages authentication services between users (by using their PEIG®), target applications and target systems. It also provides electronic identity services that are essential for authentication services. AIM can be managed via the **UIM** interface. UIM provides an easy way to manage identities and ADUCID® security parameter settings. UIM can be used to authenticate AIM by administrators, as well as by users. The number of options shown depends on the assigned role of the end-user.

1.4. 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 electronic 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.

1.5. 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 electronic identity allows us to use verified information about the physical identity.

Pairing key is a random unique string generated by the administrator and provided 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. The pairing key 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 created. It is used for identity proofing when the user's cybernetic identity is paired with their physical identity.

User profile is data about a user, such as personal data and unique identificators in external applications. This data can be saved directly on AIM or can be obtained indirectly from links to external sources (LDAP, MSAD, etc.).

1.6. ADUCID® technical terms

PEIG® proxy is a communication module that enables the client part of the target application to connect to PEIG® and also protects PEIG® as an application firewall. It must be run on the same computer as the client part of the application.

Client/server adapter is additional software for the client/server part of the application, and it enables integration of ADUCID® authentication with the application.

ADUCID® interface is a publicly defined interface between the ADUCID® system and the outside world.

2. List of activities and roles in UIM

For each particular identity provider, the whole ADUCID® system is managed via a central AIM device. This AIM can be configured and managed via the UIM component.

2.1. Standard UIM activities

UIM is used for the following activities:

- Management of members with management roles
- User management (creating, validating, changing, temporarily disabling, deleting)
- Configuration of ADUCID® service security parameters
- Management of your own identity
- Used licences statistics monitoring

2.2. Standard UIM roles

There are five standard user roles in UIM:

- ADUCID Server Kit Administrator
- Role Manager
- User Manager
- Security Manager
- End User/User

2.3. Role description

Each role is allowed to perform certain operations. The following is a list of roles and their competencies.

Role	Description
ADUCIDServerKit Administrator	Used for ADUCID Server Kit installation
Role Manager	**Management of members with roles** • Authorized to add/remove other users to/from roles

User Manager	**User management:** • Creating, changing and removing user profiles and data • Performing identity proofing • Validating users • Via pairing key • Via the registration form • Verifying and validating user data • Temporary activation/deactivation of users • Temporary activation/deactivation of PEIG®s separately
Security Manager	**Configuration of ADUCID® services security parameters** • Security profiles: • Parameters of identity validity • UKP parameters • Security profile priority • Security parameters change enforcement • Used licences statistics monitoring
(End) User	Authorized to use UIM for basic operations, including change, renew and delete their profile

Table 2-1 Standard UIM roles

3. First UIM user

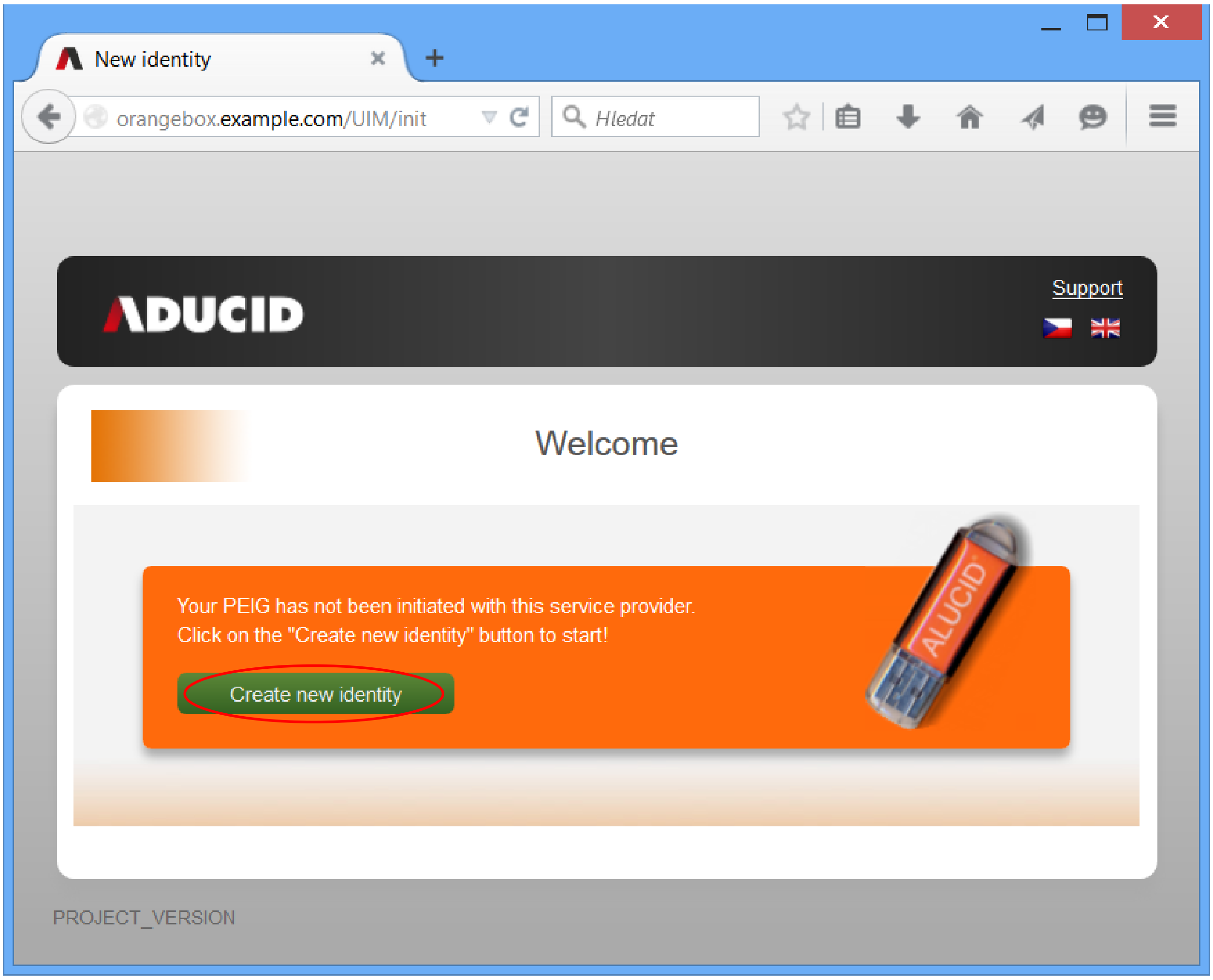
After AIM is installed, the first user to create a cybernetic identity via UIM automatically has all of the manager roles. This is called the “right for the first night.” Once the first user creates an identity in AIM, this default mechanism is deactivated for other cybernetic identities.

Note: *If you lose this first identity before you create other identities in manager roles, it is not possible to have unrestricted access rights again! The only thing you can do in this situation is to reinstall AIM completely.*

For the first log in, activate your PEIG® and go to the installed UIM via your web browser. For the UIM address, use the address that you entered during AIM installation. This guide will consistently use the following example for the UIM link: http://orangebox.example.com/UIM or https://orangebox.example.com/UIM.

If you access this address via http, you will be forwarded to a secure https channel.

1. Enter your UIM address.
2. Click **Create new identity**.



Your PEIG has not been initiated with this service provider.
Click on the "Create new identity" button to start!

Figure 3-1 Create new identity

3. PEIG® will display identification of the AIM for the identity that was created.

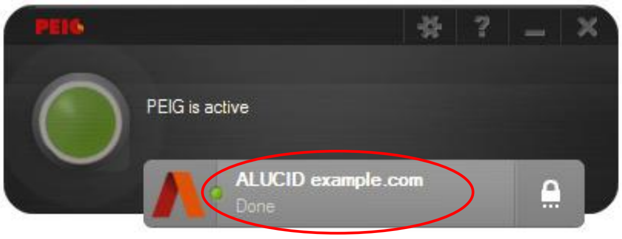
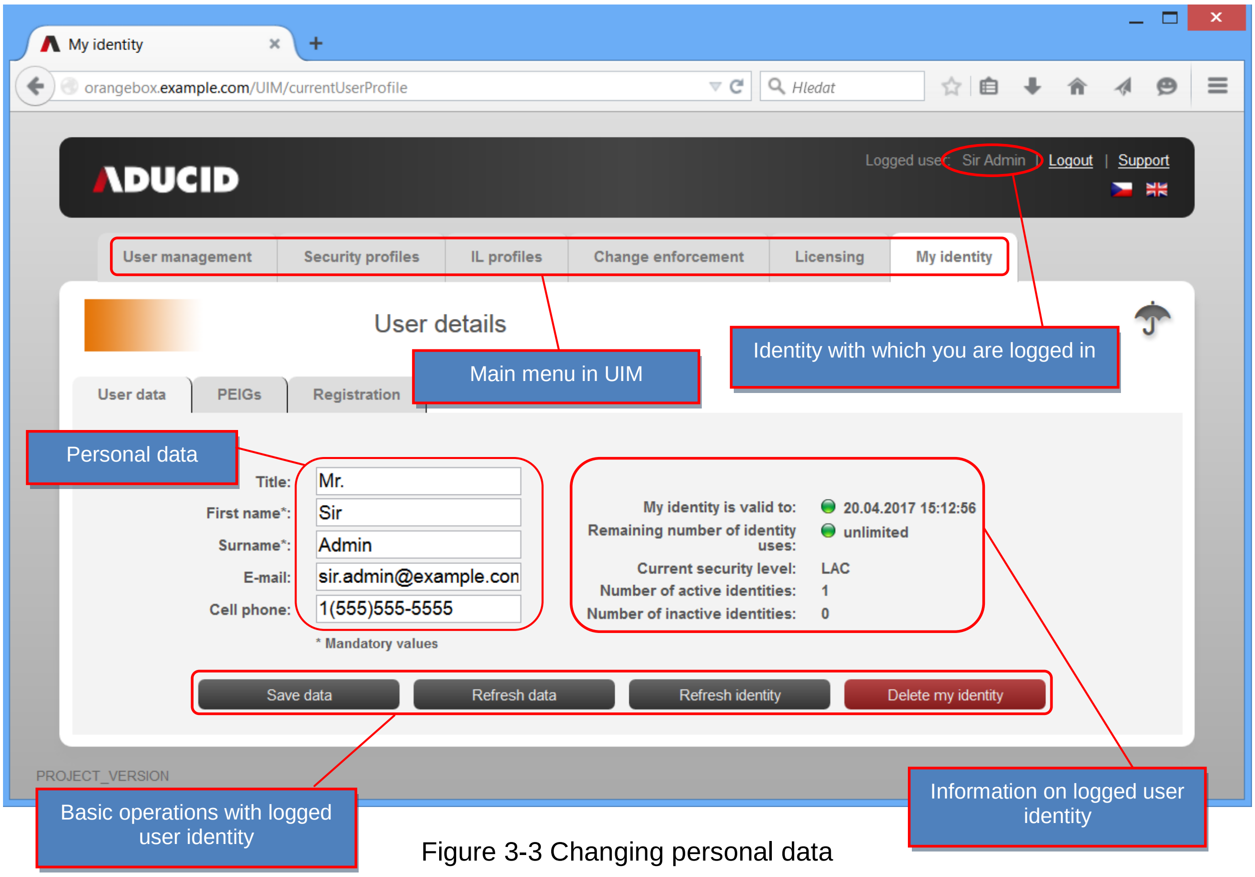


Figure 3-2 PEIG® after new identity creation

4. Now, your first UIM cybernetic identity is created and you can assign roles. Go to the **My identity** tab, enter your data, click **Save data**, and confirm the change.

How to work with the tool is described in Figure 3-5.



Title: Mr.
First name*: Sir
Surname*: Admin
E-mail: sir.admin@example.con
Cell phone: 1(555)555-5555
* Mandatory values

My identity is valid to: ● 20.04.2017 15:12:56
Remaining number of identity uses: ● unlimited
Current security level: LAC
Number of active identities: 1
Number of inactive identities: 0

Figure 3-3 Changing personal data

4. Managing membership in user manager roles

Only a Role Manager can add or remove roles for other users. If you wish to delegate these activities to other users, you need to add them to the Role Manager group.

To add/remove a user to/from a role, do the following:

1. Log in to UIM with PEIG®.
2. Switch to the **Users** tab.
3. Select **Search users**.
4. Click on the user name.
5. In the **User role** section, select the required roles for the user. If you wish to select more options, press the **CTRL** key and click additional roles.
6. Click **Save changes** to confirm the changes.

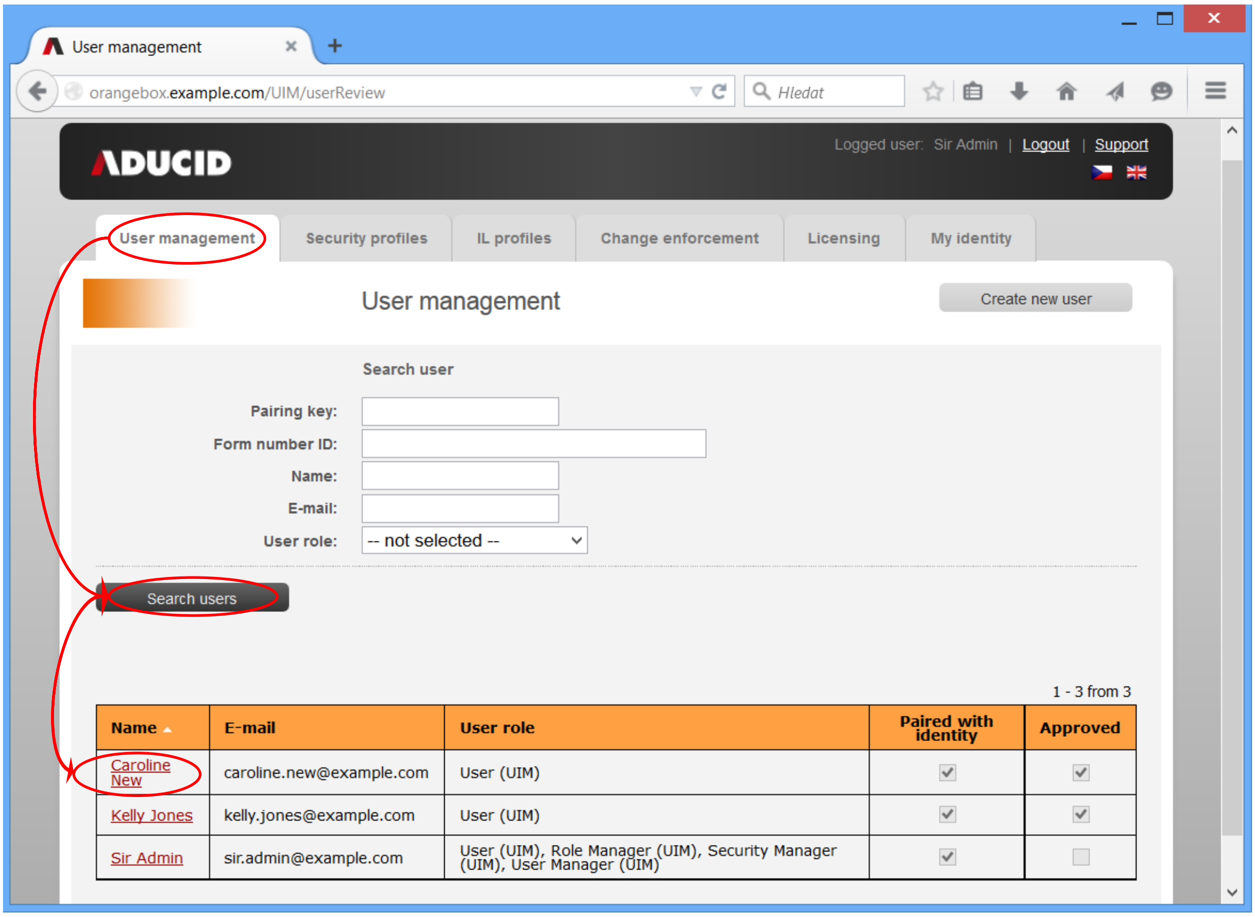
5. User management

User management consists of the following activities:

- Creating, changing and removing user profiles
- Performing identity proofing
- Validating users
  - Via the pairing key
  - Via the registration form
- Verifying and validating user data
- Temporary activation/deactivation of users
- Temporary activation/deactivation of PEIG®s separately

5.1. Creating, changing and removing other users (their profiles/data)

1. Log in with your PEIG®.
2. Click the **User management** tab, select **Search users**, and then click on the user profile that you are going to modify.



Search user

Pairing key:	
Form number ID:	
Name:	
E-mail:	
User role:	-- not selected --

1 - 3 from 3

Name ▲	E-mail	User role	Paired with identity	Approved
Caroline New	caroline.new@example.com	User (UIM)	☑	☑
Kelly Jones	kelly.jones@example.com	User (UIM)	☑	☑
Sir Admin	sir.admin@example.com	User (UIM), Role Manager (UIM), Security Manager (UIM), User Manager (UIM)	☑	□

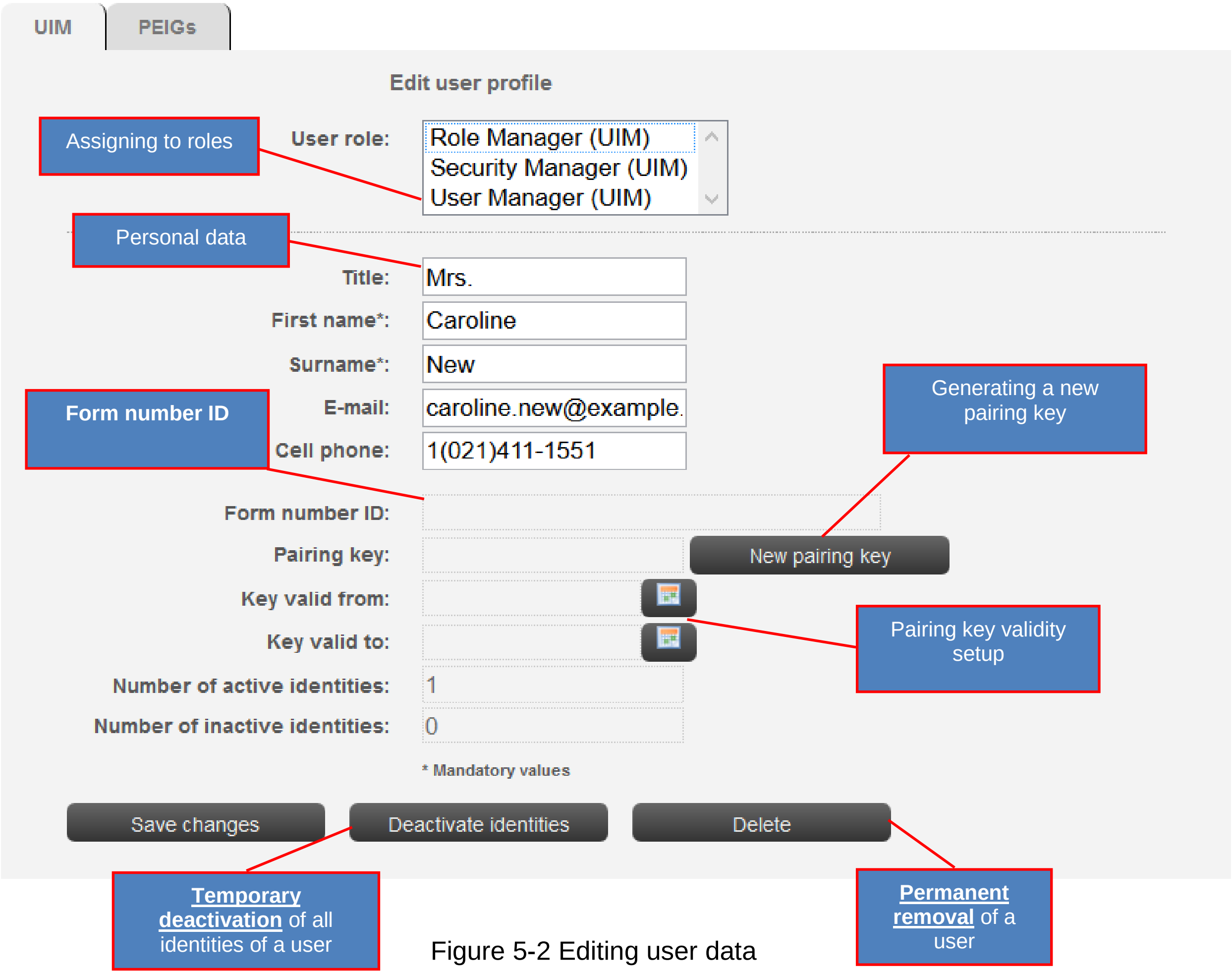
Figure 5-1 User management

- For efficient searching, enter a precise string into the search field. For example, when searching for user names, you can use the asterisk wildcard.

3. Update the data in the user profile as needed.

On the “UIM” tab you can:

- Define user roles
- Modify a users’ personal data
- Generate a new pairing key and change validity for a user
- Check how many cybernetic identities the user has and how many of them are:
  - enabled
  - disabled
- Activate and deactivate user identities:
  - Activated user identity = the user can use this identity and is allowed to log in
  - Deactivated user identity = the user cannot use this identity and is not allowed to log in


UIM
PEIGs
Assigning to roles
Personal data
Form number ID
Generating a new pairing key
Pairing key validity setup
Temporary deactivation of all identities of a user
Permanent removal of a user
New pairing key
Save changes
Deactivate identities
Delete

Edit user profile

User role:	Role Manager (UIM) Security Manager (UIM) User Manager (UIM)
Title:	Mrs.
First name*:	Caroline
Surname*:	New
E-mail:	caroline.new@example.
Cell phone:	1(021)411-1551
Form number ID:	
Pairing key:	
Key valid from:	
Key valid to:	
Number of active identities:	1
Number of inactive identities:	0

* Mandatory values

Figure 5-2 Editing user data

On the “PEIGs” tab you can:

- Temporary activate/deactivate PEIG®s separately

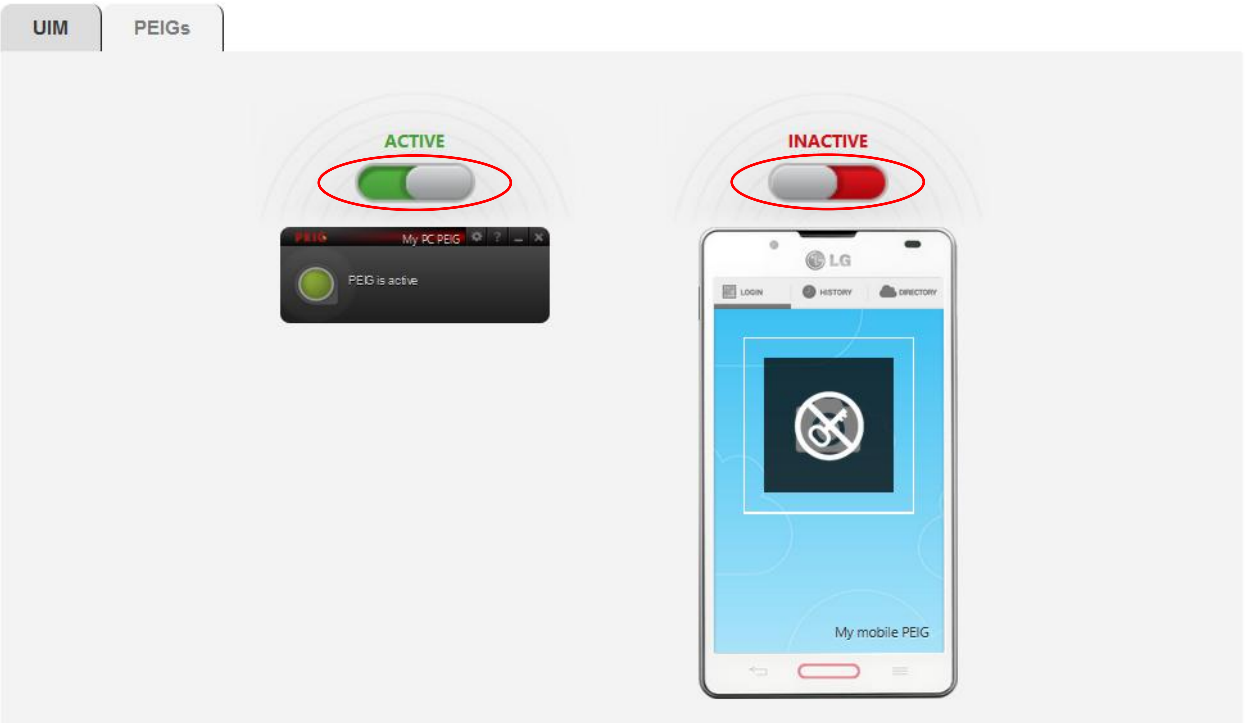


Figure 5-3 Activation/deactivation PEIG®s separately

4. Click **OK** to confirm changes – valid only fro the first tab “UIM”.

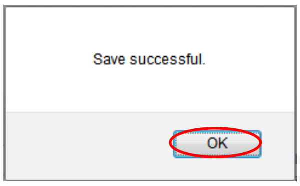

Save successful.

Figure 5-4 Notification

5.2. Creating a new ADUCID® user

All new profiles must be created in the ADUCID® system, by using AIM.

This can be done in three steps. The order of the first two steps may depend on the scenario used.

- Creating user’s cybernetic identity in AIM
- Entering user’s personal data into AIM
- Identity proofing and pairing the user’s cybernetic identity with a matching user profile

By default, the UIM application supports two scenarios for creating a user in AIM.

Scenario 1 – Pairing key:

- The User Manager creates a profile for a new user
- The new user creates their cybernetic identity
- The new user links this new cybernetic identity to their profile

Scenario 2 – Registration form:

- A new user creates a new cybernetic identity
- The new user creates a new user profile by using the registration form
- The User Manager verifies the user by:
  - Verifying that the data are correct

  - Verifying that the form is from the person whose data are presented in the form
- The User Manager validates the new user in UIM

5.2.1. Scenario 1 – “Pairing key”

The process of creating a user’s identity in the system by using the pairing key scenario is described in Figure 5-4:

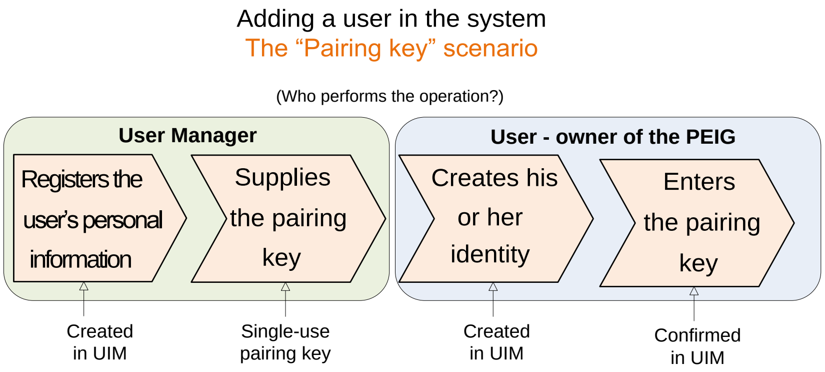

Adding a user in the system
The “Pairing key” scenario
(Who performs the operation?)
User Manager
User - owner of the PEIG
Registers the user’s personal information
Supplies the pairing key
Creates his or her identity
Enters the pairing key
Created in UIM
Single-use pairing key
Created in UIM
Confirmed in UIM

Figure 5-5 “Pairing key” scenario

Steps to be taken:

User Manager	1. Log in to UIM. 2. Create a user profile in UIM. 3. Generate a pairing key. 4. Provide the pairing key to the user.
New user	1. Start and activate your PEIG®. 2. Create your new cybernetic identity in UIM. 3. Enter your pairing key.

Prerequisites:

- The user has a PEIG® that is running and active
- The user has no cybernetic identity with the particular identity provider
- The user’s Manager is a member of the User Manager group

Procedure:

1. The User Manager logs in to UIM.
2. The User Manager goes to the **User Management** tab and clicks **Create new user**.

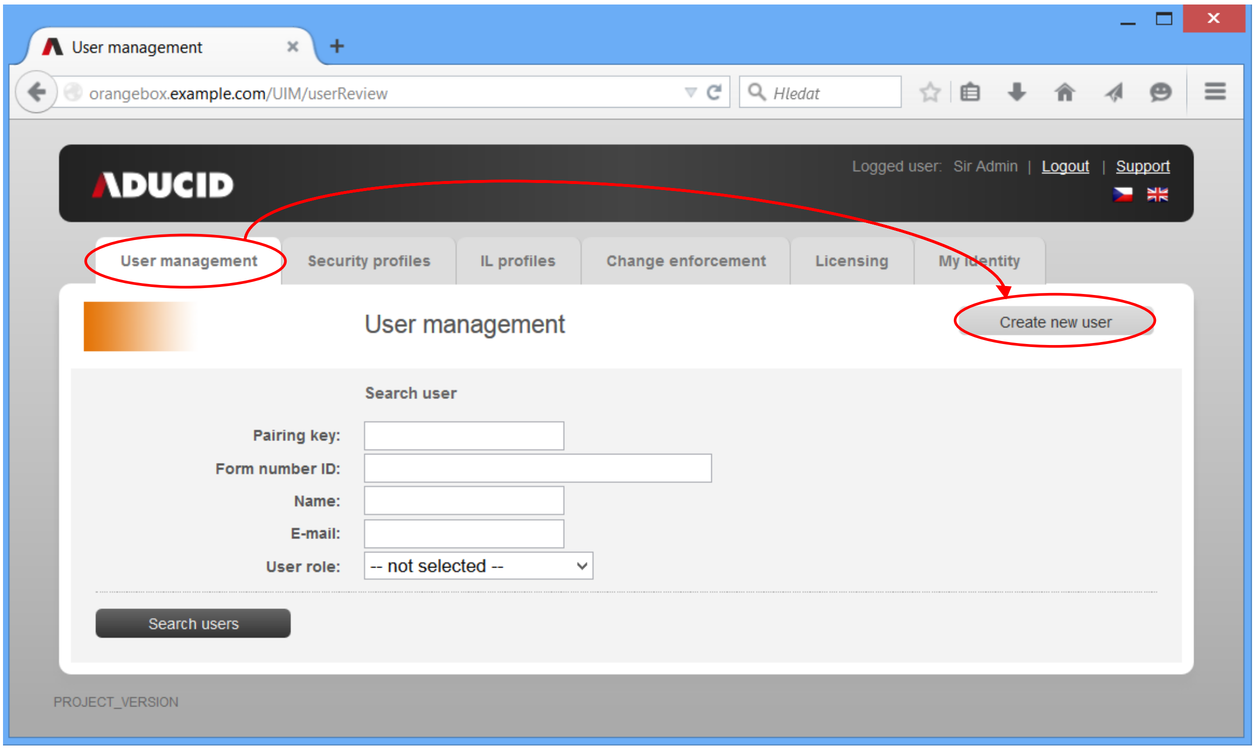
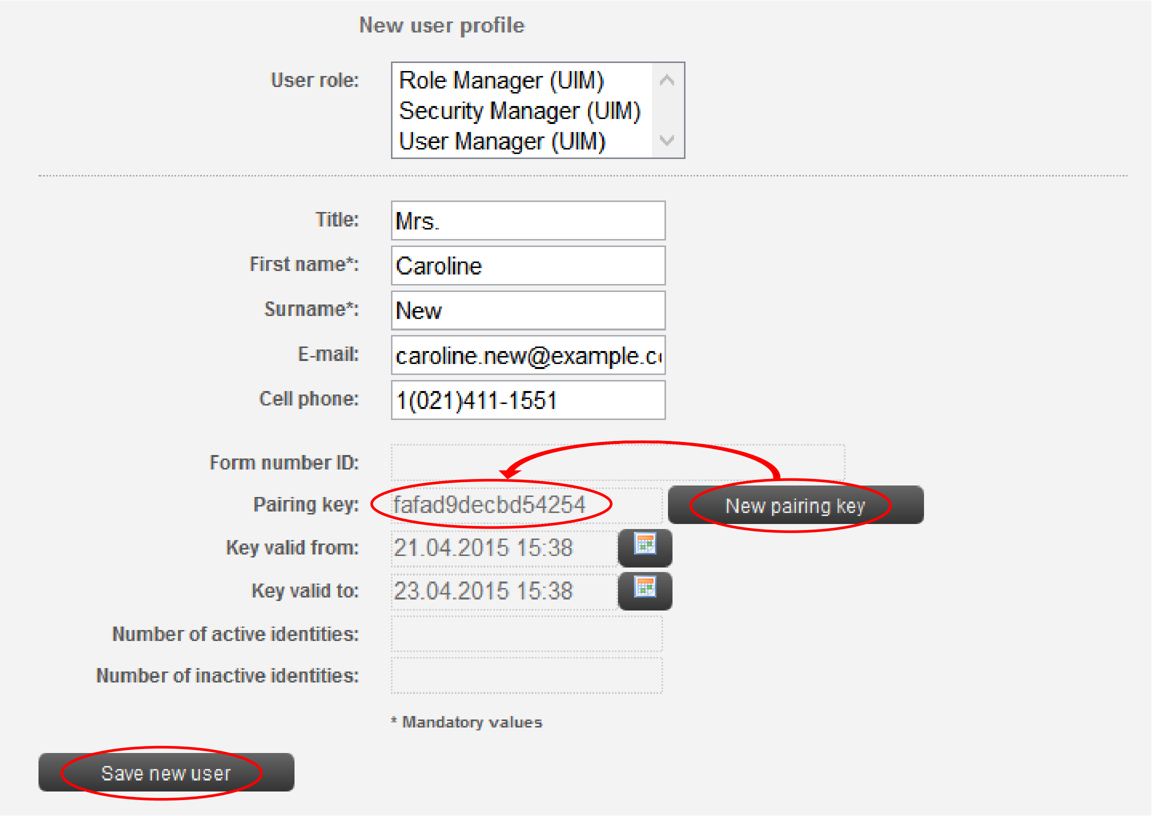


Figure 5-6 Create new user

3. The User Manager enters the information about the new user and generates a new pairing key for the user (or updates the validity, as necessary).

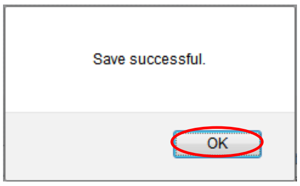


New user profile

User role:	Role Manager (UIM) Security Manager (UIM) User Manager (UIM)
Title:	Mrs.
First name*:	Caroline
Surname*:	New
E-mail:	caroline.new@example.c
Cell phone:	1(021)411-1551
Form number ID:	
Pairing key:	fafad9decbd54254
Key valid from:	21.04.2015 15:38
Key valid to:	23.04.2015 15:38
Number of active identities:	
Number of inactive identities:	

Figure 5-7 Generating new pairing key

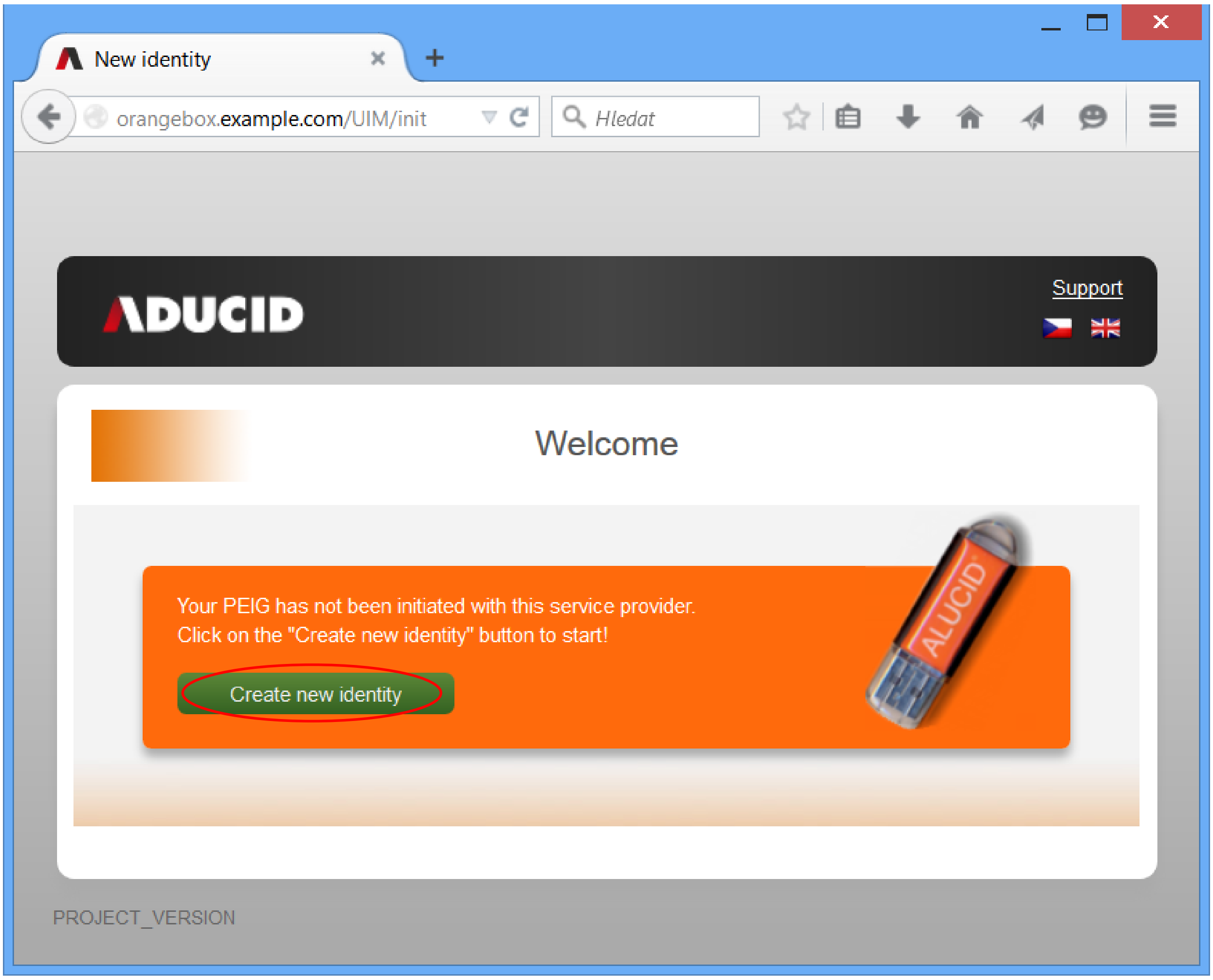
4. The User Manager clicks **Save new user**.



Save successful.

Figure 5-8 Notification

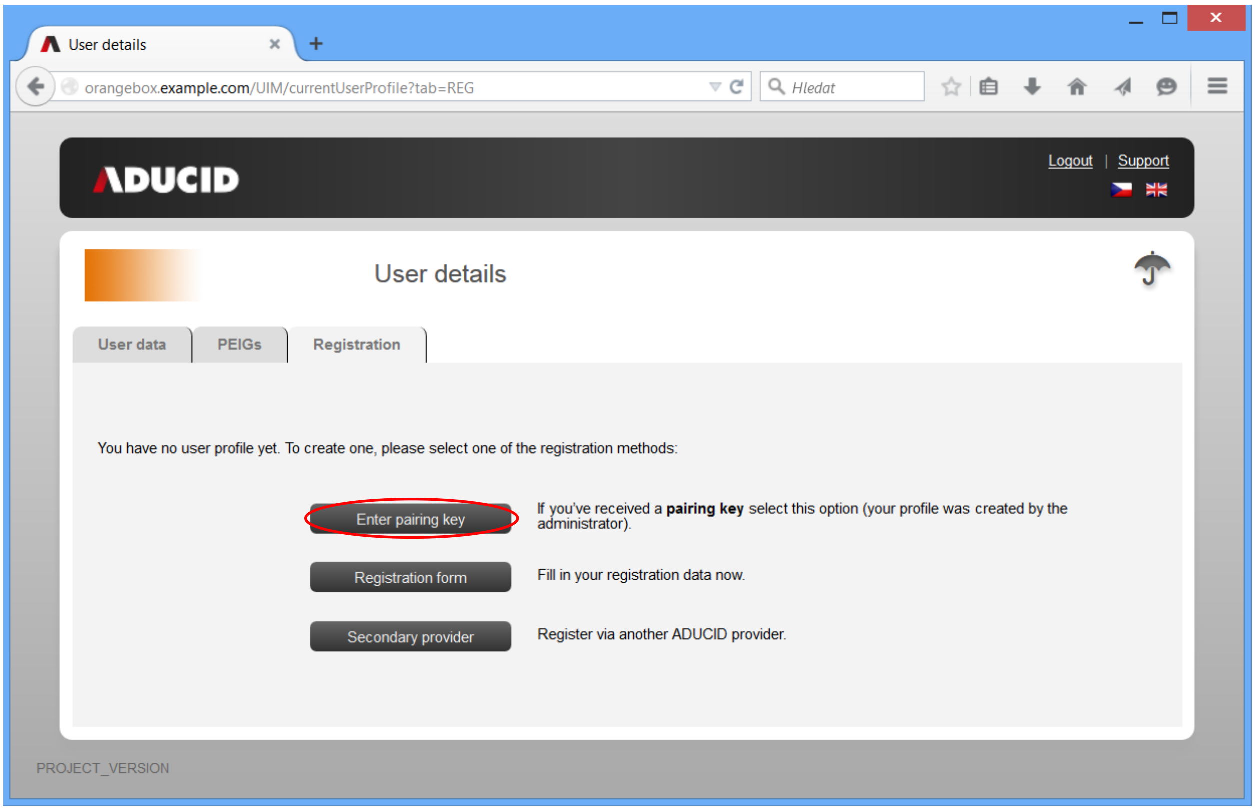
5. The User Manager securely provides the pairing key to the new user.
6. The new user starts and activates their PEIG®.
7. The new user logs in to UIM.
8. The new user creates a new identity. The user clicks **Create new identity**. In case, the current security profile has direct init set, page on the page below will not appear and identity will be initialized automatically.



Your PEIG has not been initiated with this service provider.
Click on the "Create new identity" button to start!

Figure 5-9 Create new identity

9. The new user clicks **Enter pairing key**.



You have no user profile yet. To create one, please select one of the registration methods:

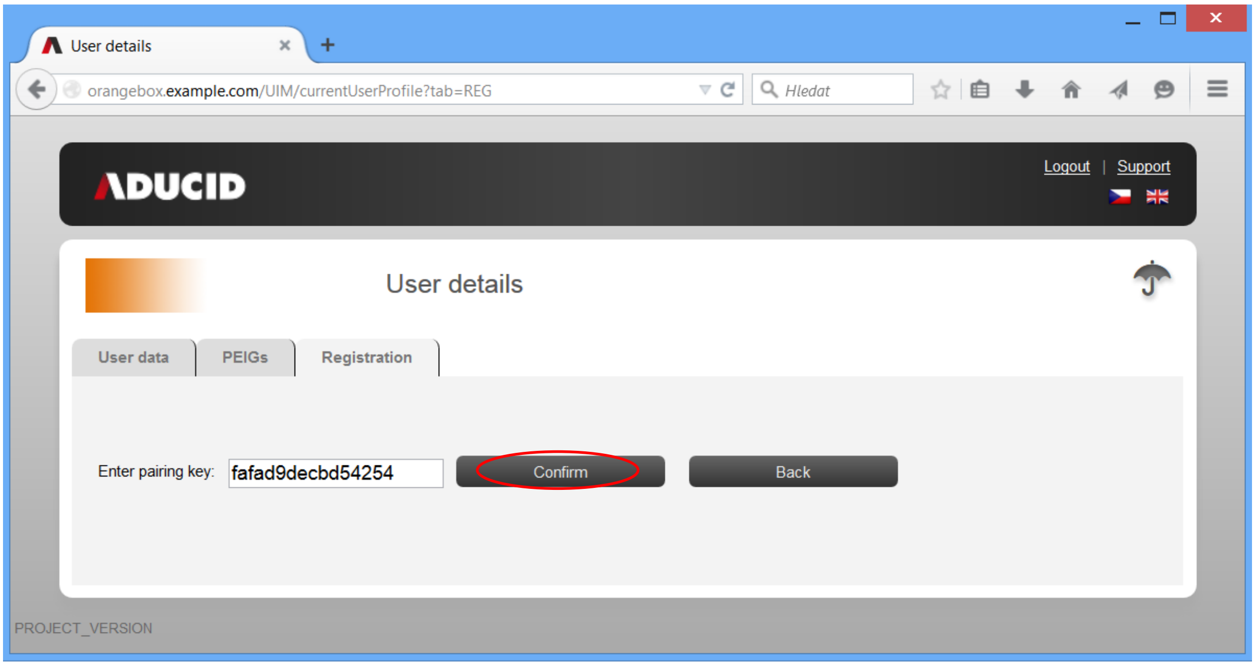
If you've received a **pairing key** select this option (your profile was created by the administrator).

Fill in your registration data now.

Register via another ADUCID provider.

Figure 5-10 Creating user by using pairing key

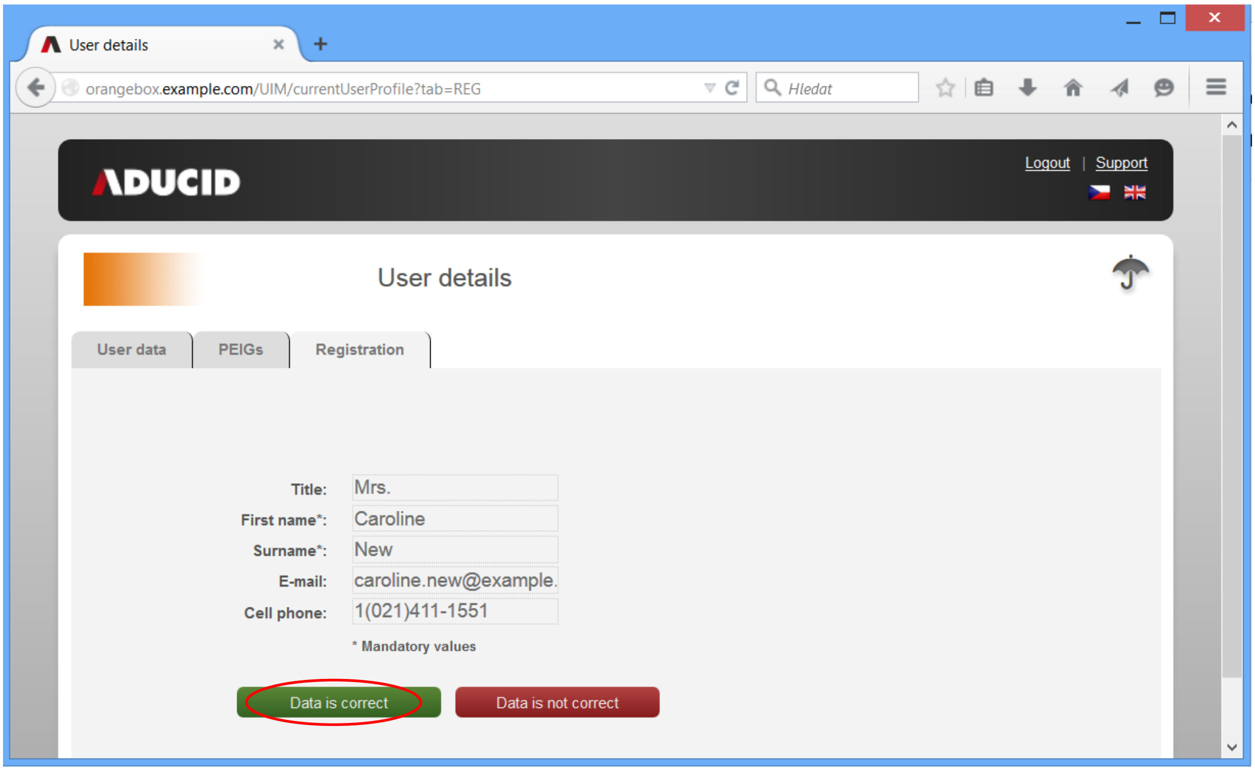
10. The user enters the received pairing key and clicks **Confirm**.



Enter pairing key: fafad9decbd54254

Figure 5-11 Pairing key

11. If the data displayed are correct, the new user confirms this by clicking **Data are correct**. If not, they click **Data are incorrect**.



Title: Mrs.

First name*: Caroline

Surname*: New

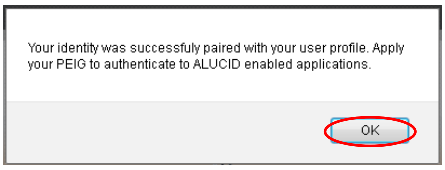
E-mail: caroline.new@example.

Cell phone: 1(021)411-1551

* Mandatory values

Figure 5-12 Data validation

12. The registration procedure is complete.

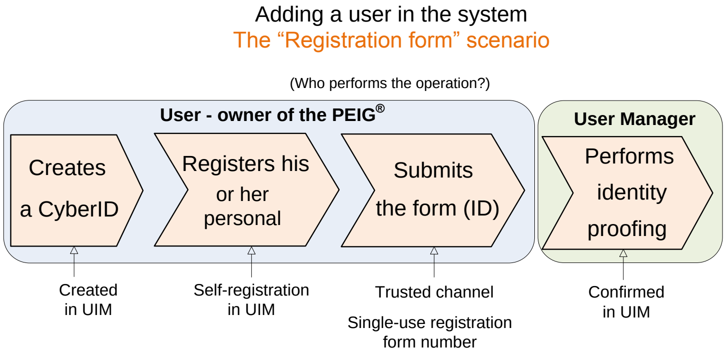


Your identity was successfuly paired with your user profile. Apply your PEIG to authenticate to ALUCID enabled applications.

Figure 5-13 Notification

5.2.2. Scenario 2 – “Registration form”

The following describes how to create an identity by using the registration form.

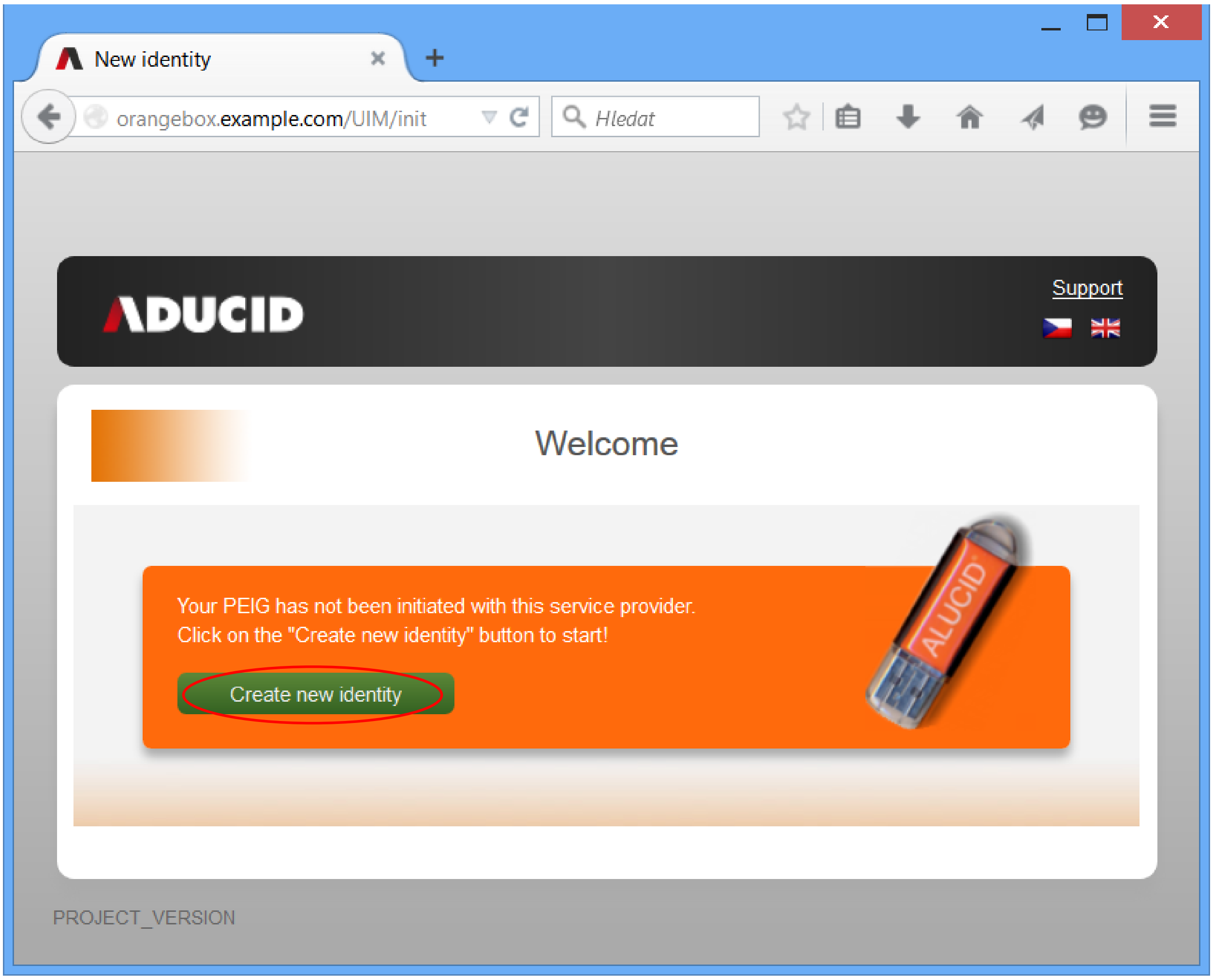


Adding a user in the system
The “Registration form” scenario
(Who performs the operation?)
User - owner of the PEIG®
Creates a CyberID
Registers his or her personal
Submits the form (ID)
User Manager
Performs identity proofing
Created in UIM
Self-registration in UIM
Trusted channel
Single-use registration form number
Confirmed in UIM

Figure 5-14 Registration form scenario

New user	1. Create your new cybernetic identity. 2. Enter your personal data on the registration form. 3. Provide the form number to the User Manager.
User Manager	1. Use the number of the registration form to find the user in UIM. 2. Verify the user via **identity proofing**. 3. Verify that the data entered in the form are correct. 4. Validate the user in UIM.

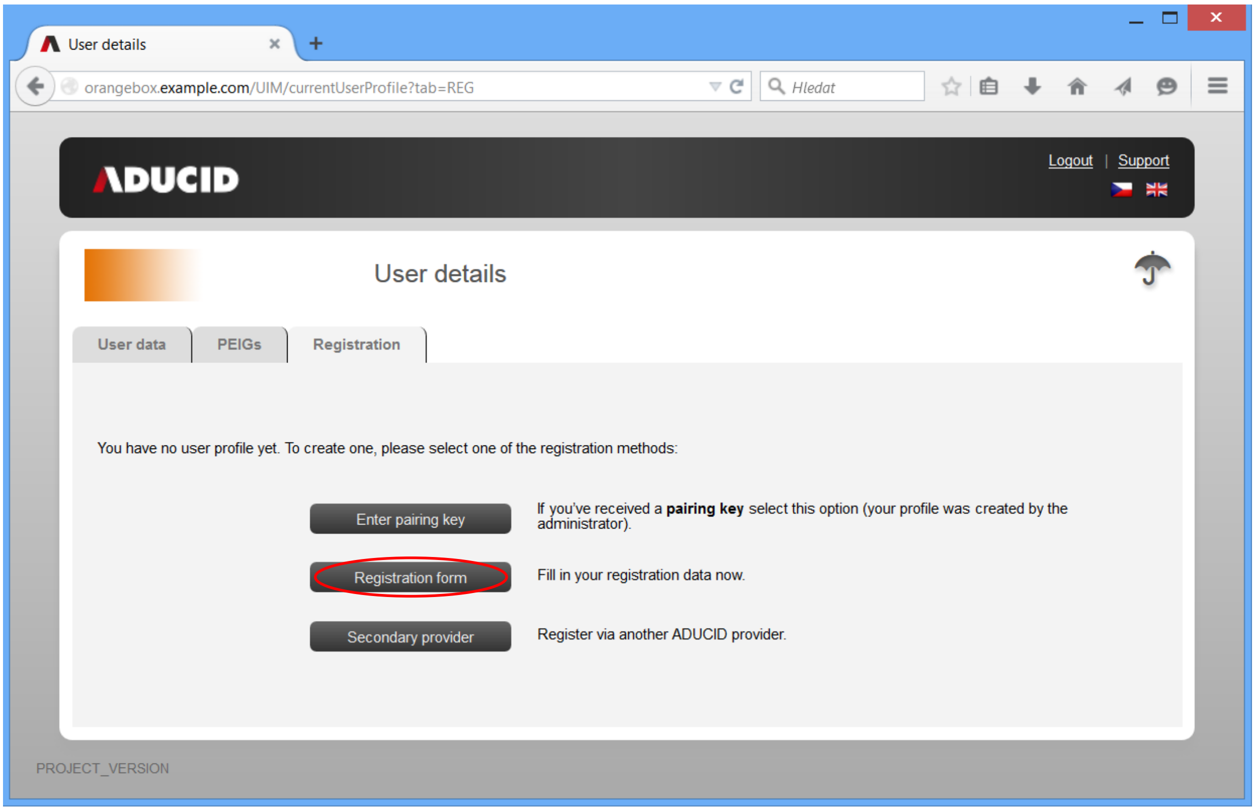
1. The new user logs in to UIM https://orangebox.example.com and creates a new cybernetic identity. In case, the current security profile has direct init set, page on the page below will not appear and identity will be initialized automatically.



Your PEIG has not been initiated with this service provider.
Click on the "Create new identity" button to start!

Figure 5-15 Create new identity

2. The user clicks **Registration form**.



You have no user profile yet. To create one, please select one of the registration methods:

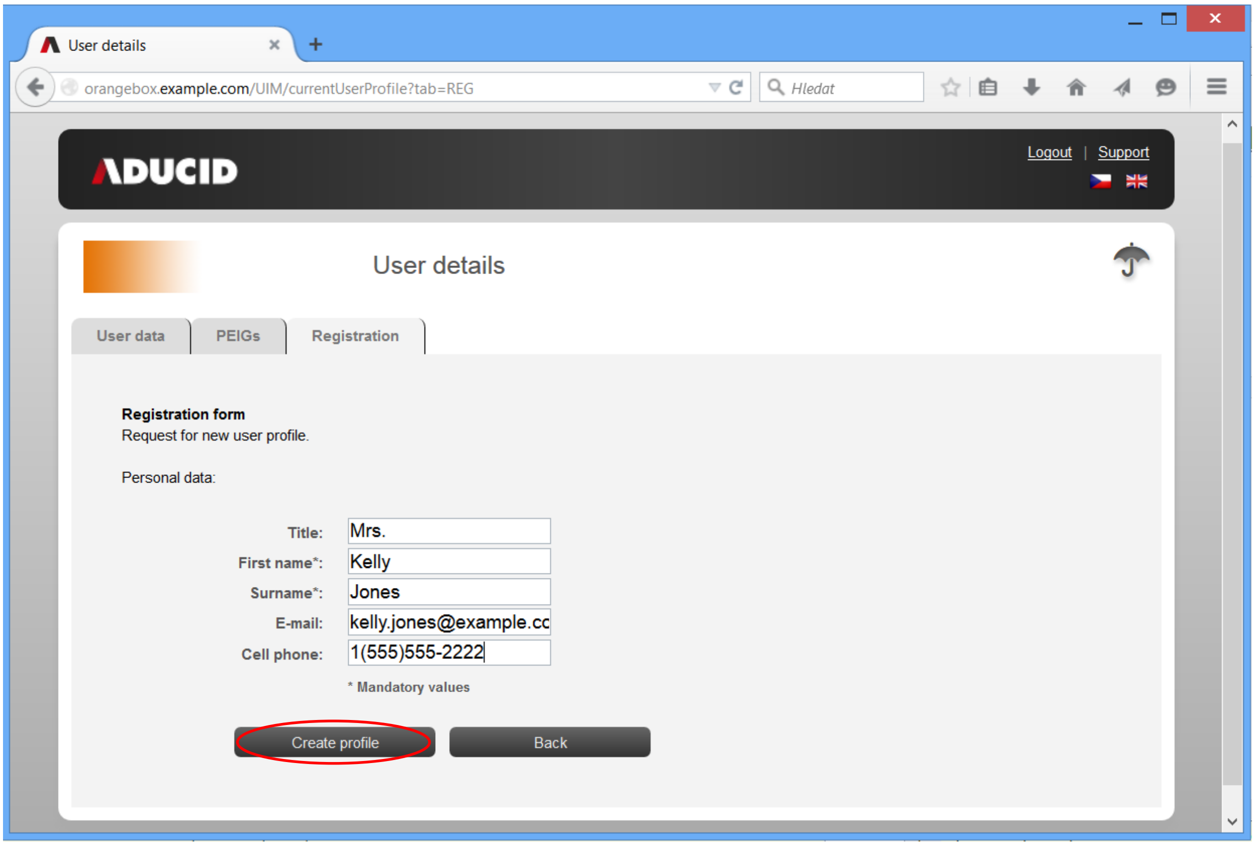
Enter pairing key — If you've received a **pairing key** select this option (your profile was created by the administrator).

Registration form — Fill in your registration data now.

Secondary provider — Register via another ADUCID provider.

Figure 5-16 Select Registration form

3. The user enters and confirms their data.



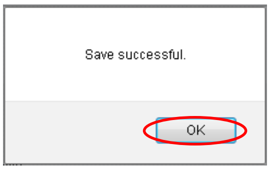
Registration form
Request for new user profile.

Personal data:

Title:	Mrs.
First name*:	Kelly
Surname*:	Jones
E-mail:	kelly.jones@example.cc
Cell phone:	1(555)555-2222

* Mandatory values

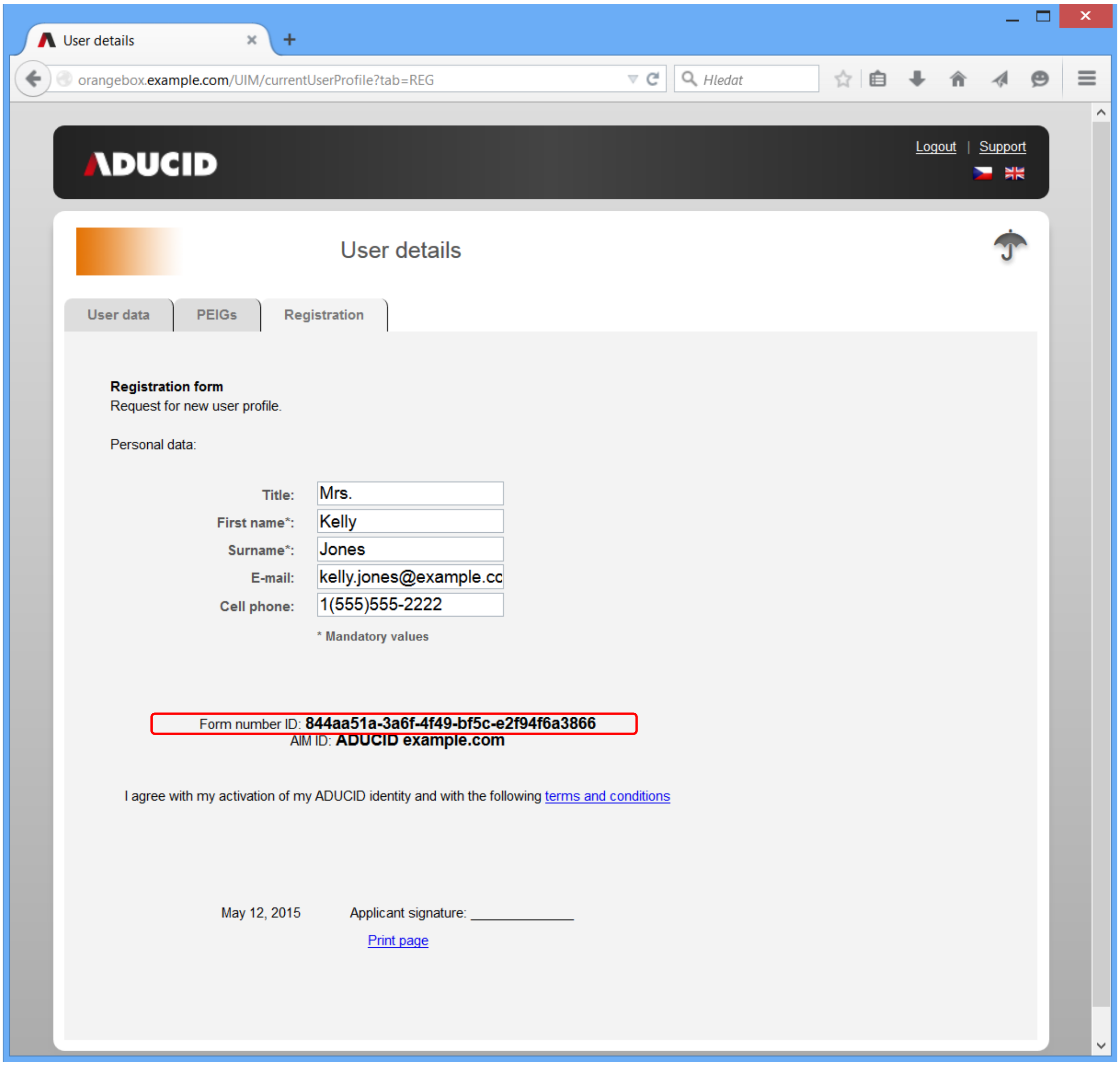
Figure 5-17 Confirmation



Save successful.

Figure 5-18 Notification

4. The user prints the form displayed and provides the form number to the User Manager.



Registration form
Request for new user profile.

Personal data:

Title:	Mrs.
First name*:	Kelly
Surname*:	Jones
E-mail:	kelly.jones@example.cc
Cell phone:	1(555)555-2222

* Mandatory values

Form number ID: **844aa51a-3a6f-4f49-bf5c-e2f94f6a3866**
AIM ID: **ADUCID example.com**

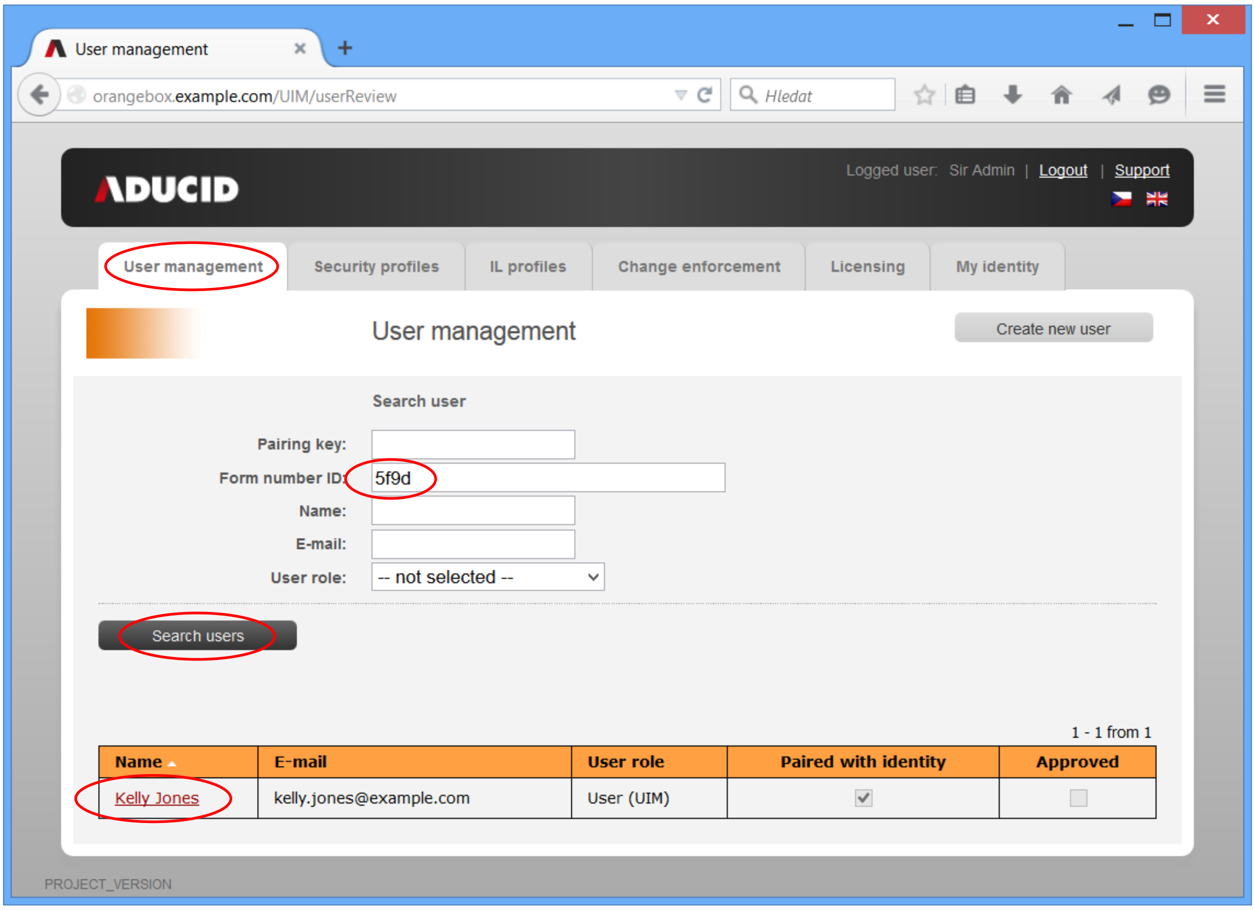
I agree with my activation of my ADUCID identity and with the following terms and conditions

May 12, 2015 Applicant signature: ____________

Print page

Figure 5-19 Registration form

5. The User Manager logs in to UIM, clicks **User management**, and then enters the number of the form (or a part of it) and finds the user.



Pairing key:	
Form number ID:	5f9d
Name:	
E-mail:	
User role:	-- not selected --

1 - 1 from 1

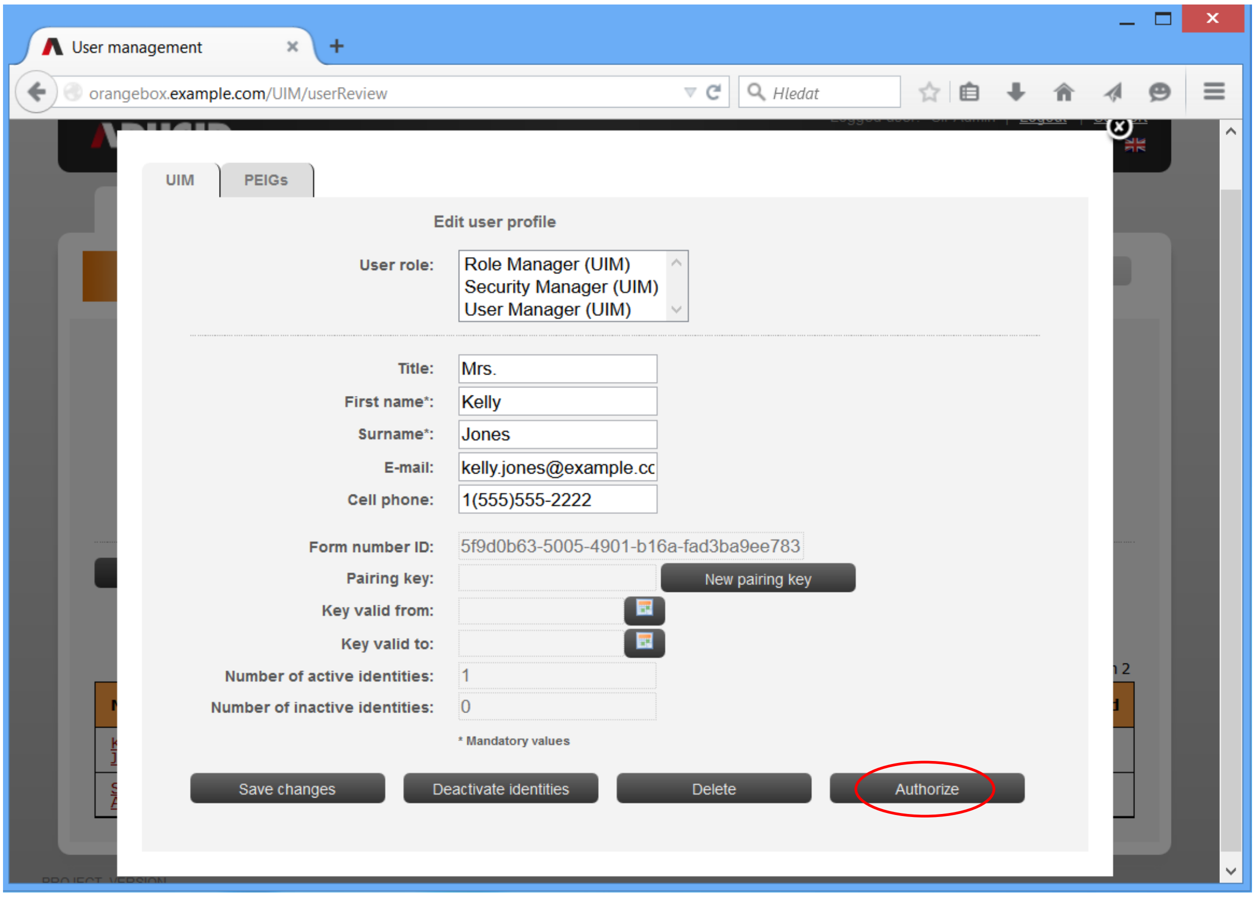
Name	E-mail	User role	Paired with identity	Approved
Kelly Jones	kelly.jones@example.com	User (UIM)	☑	□

Figure 5-20 Search users using registration form

6. User Manager:

- Verifies the whole number of the form
- Verifies the data about the particular user

If everything is OK, the User Manager validates the user by clicking **Authorize**.

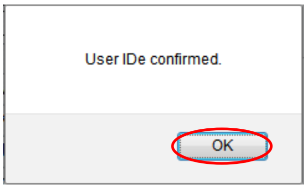


Edit user profile

User role:	Role Manager (UIM) Security Manager (UIM) User Manager (UIM)
Title:	Mrs.
First name*:	Kelly
Surname*:	Jones
E-mail:	kelly.jones@example.cc
Cell phone:	1(555)555-2222
Form number ID:	5f9d0b63-5005-4901-b16a-fad3ba9ee783
Pairing key:	
Key valid from:	
Key valid to:	
Number of active identities:	1
Number of inactive identities:	0

* Mandatory values

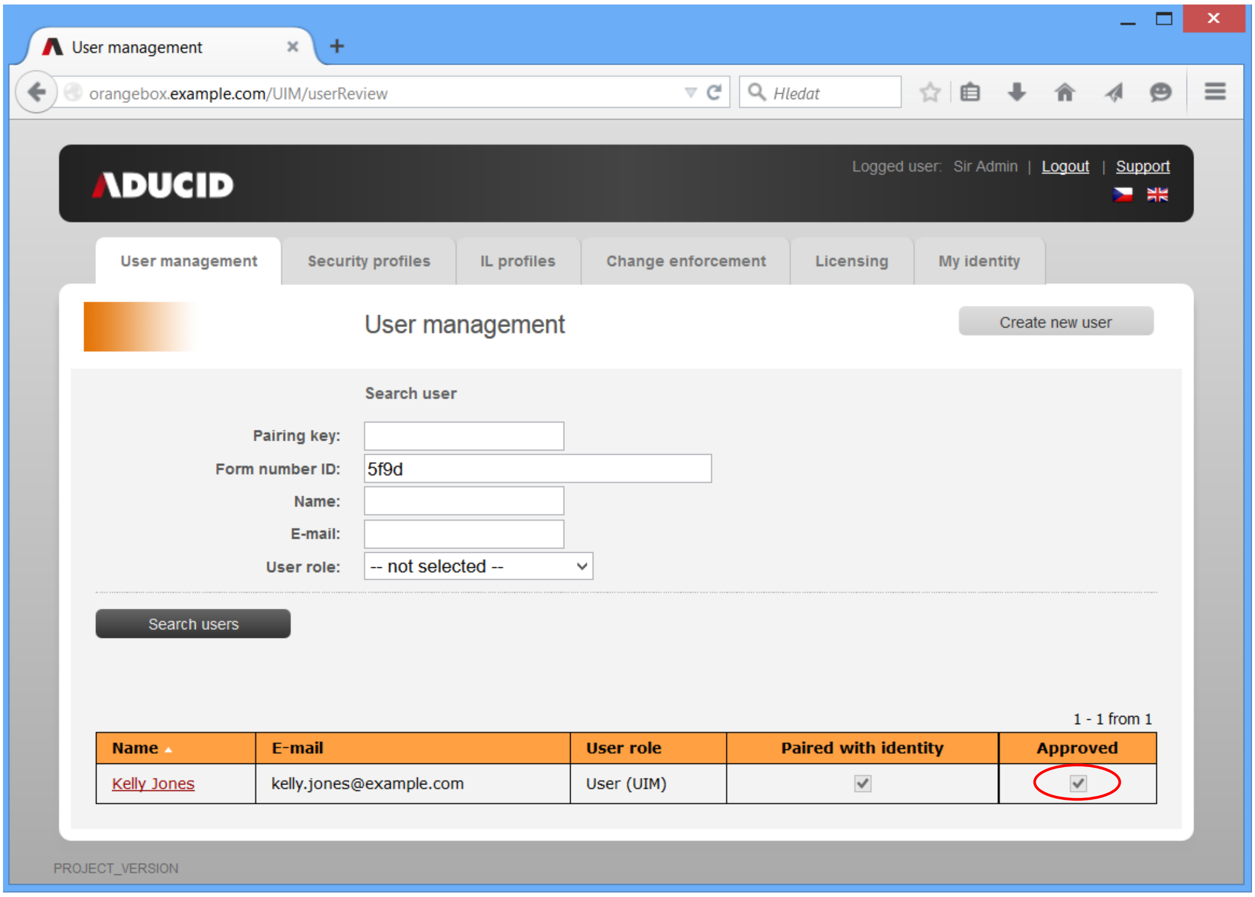
Figure 5-21 Authorization



User IDe confirmed.

Figure 5-22 Notification

7. The User Manager verifies that the particular user has been authorized.



User management

Search user

Pairing key:	
Form number ID:	5f9d
Name:	
E-mail:	
User role:	-- not selected --

Search users

1 - 1 from 1

Name ▲	E-mail	User role	Paired with identity	Approved
Kelly Jones	kelly.jones@example.com	User (UIM)	☑	☑

Figure 5-23 Verification

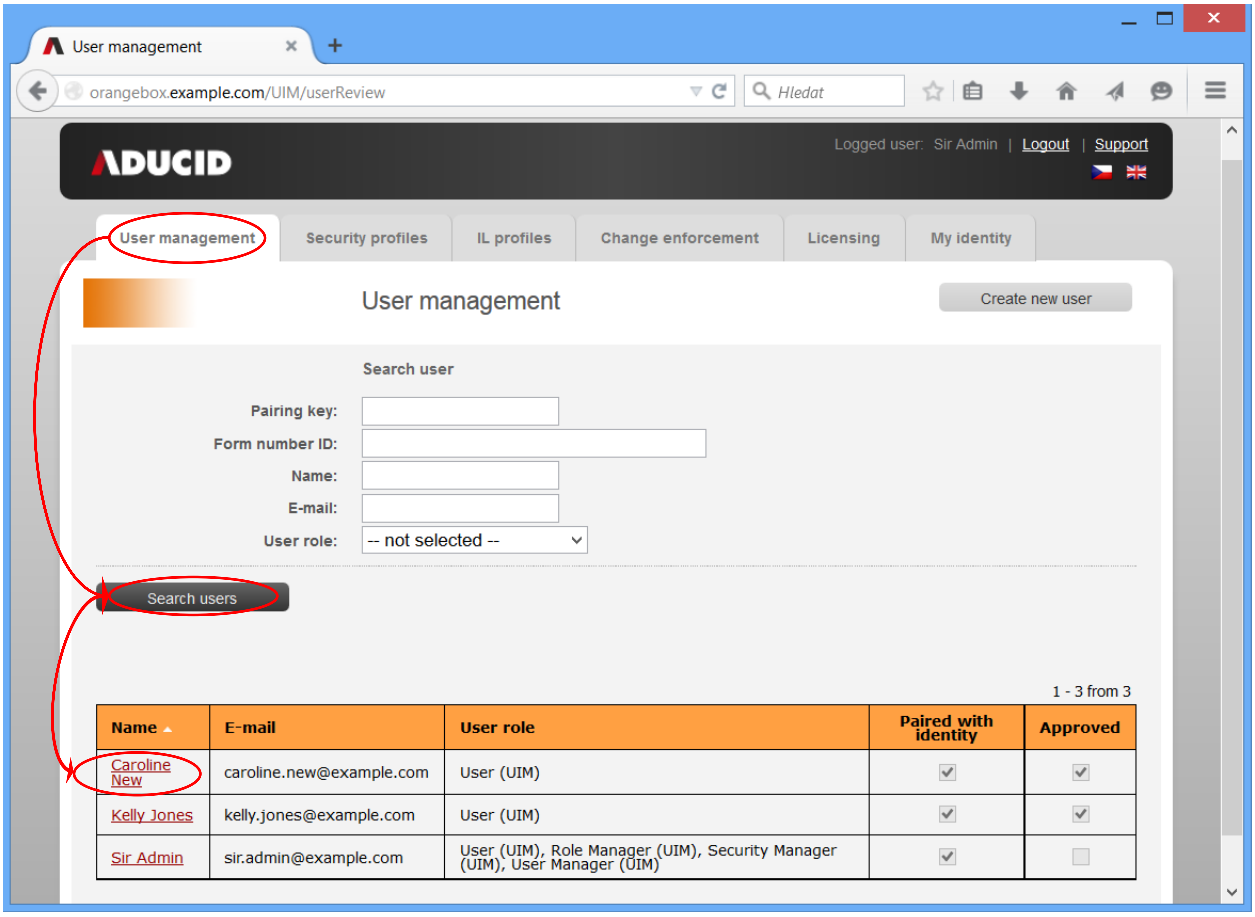
5.3. Temporary activation and deactivation of users

The User Manager can temporarily disable all cybernetic identities by using UIM.

The blocked identities can be re-enabled by the User Manager.

5.3.1. How to disable/enable identities temporarily

1. The User Manager logs in to UIM.
2. The User Manager clicks **User management** and then **Search users**.
3. The User Manager clicks on the user whose identities are to be disabled/enabled:



Search user

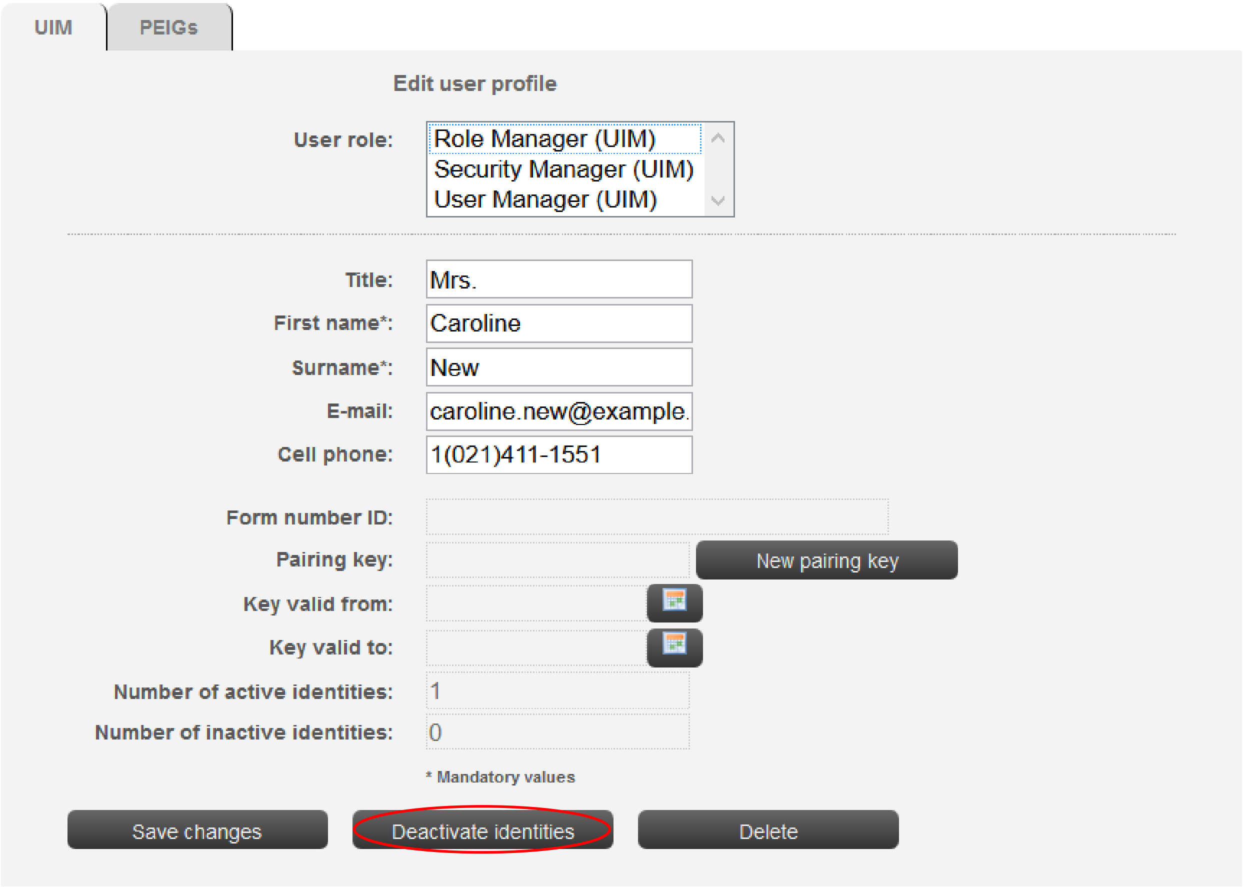
Pairing key:	
Form number ID:	
Name:	
E-mail:	
User role:	-- not selected --

1 - 3 from 3

Name	E-mail	User role	Paired with identity	Approved
Caroline New	caroline.new@example.com	User (UIM)	✓	✓
Kelly Jones	kelly.jones@example.com	User (UIM)	✓	✓
Sir Admin	sir.admin@example.com	User (UIM), Role Manager (UIM), Security Manager (UIM), User Manager (UIM)	✓	□

Figure 5-24 User management

The User Manager clicks **Deactivate identities**.



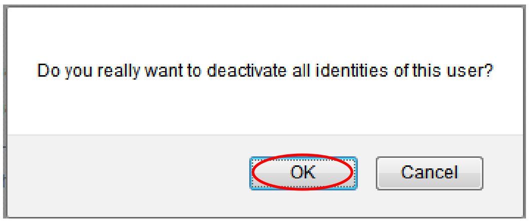
Edit user profile

User role: Role Manager (UIM)
Security Manager (UIM)
User Manager (UIM)

Title:	Mrs.
First name*:	Caroline
Surname*:	New
E-mail:	caroline.new@example.
Cell phone:	1(021)411-1551
Form number ID:	
Pairing key:	
Key valid from:	
Key valid to:	
Number of active identities:	1
Number of inactive identities:	0

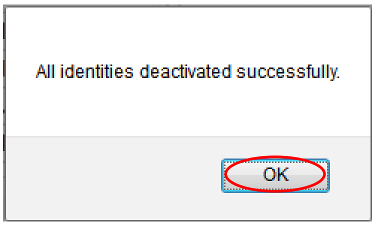
* Mandatory values

Figure 5-25 Identity deactivation



Do you really want to deactivate all identities of this user?

Figure 5-26 Deactivation confirmation



All identities deactivated successfully.

Figure 5-27 Notification

Deactivated identities can be activated in the same way; by clicking **Activate identities**, instead of **Deactivate identities**.

You can also activate and deactivate individual user identities on the “PEIGs” tab.

6. Management of ADUCID® security parameters

Management of security parameters can be done by security profiles, which contain sets of parameters.

- Management of UKP security profile parameters (universal cryptographic protocol)
- Management of IL identificator parameters (when a user's registration is being transferred from another provider)
- Enforcing changes of security parameters of all identities in a particular AIM

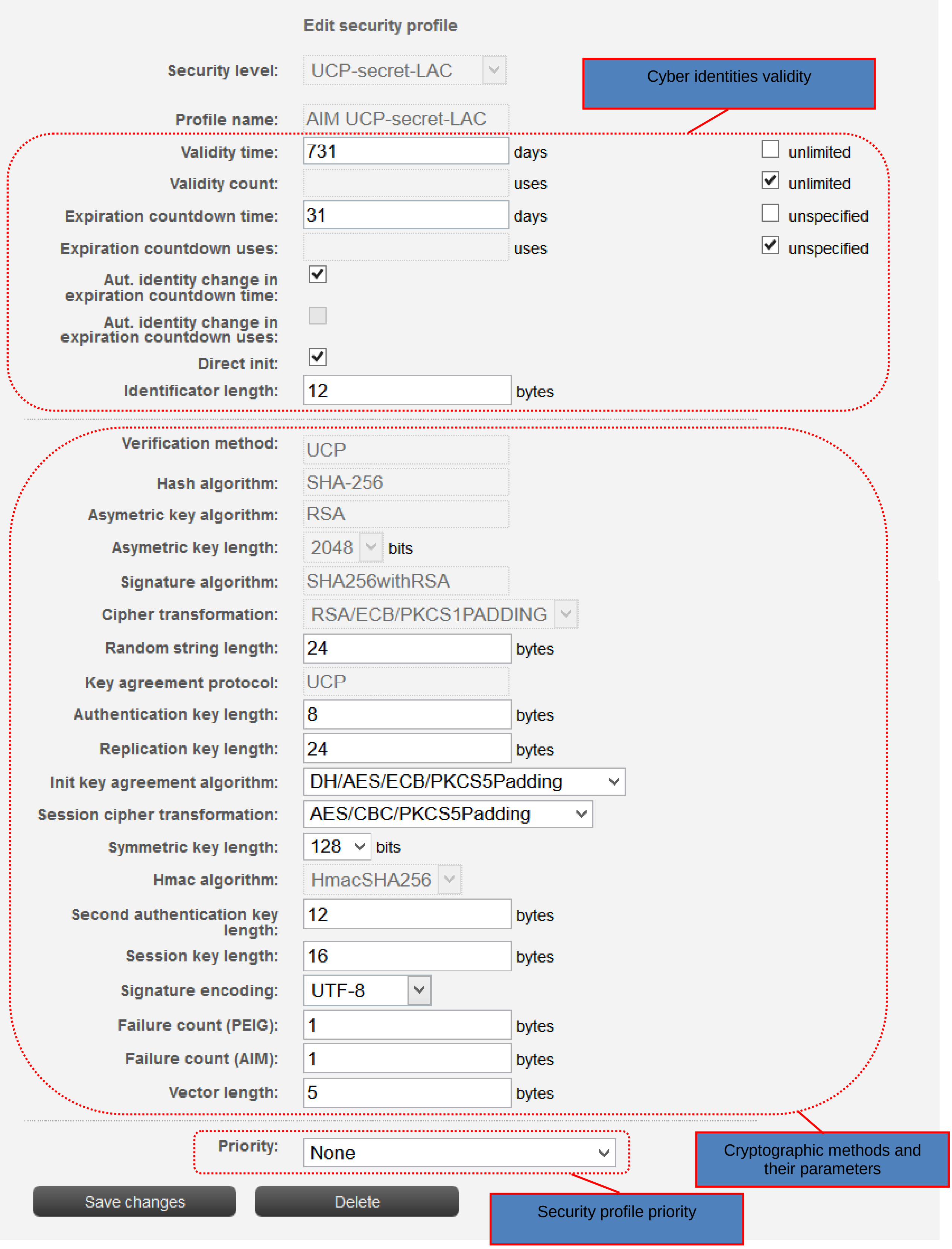
6.1. Management of UKP security profile

6.1.1. Security profile – introduction

Security profile defines and enforces security parameters for cybernetic identities in the system. In fact, it is a basic, defined set of security parameters for an identity. The security profile defines the following:

- Profile name
- Cybernetic identity validity
  - **Maximum time** (period) of identity validity
  - **Expiration countdown time** (when a user must be warned, in days, before the expiration date)
  - **Permitted number of identity uses** (how many times the identity can be used before it expires)
  - **Expiration countdown uses** (how many uses before expiration the user must be warned)
- Automated change (renewal) of identity – on/off
- Cryptographic methods and parameters

An example of parameters for UCP-secret-LAC can be found on the next page.



Edit security profile

Security level:	UCP-secret-LAC		
Profile name:	AIM UCP-secret-LAC		
Validity time:	731	days	□ unlimited
Validity count:		uses	☑ unlimited
Expiration countdown time:	31	days	□ unspecified
Expiration countdown uses:		uses	☑ unspecified
Aut. identity change in expiration countdown time:	☑		
Aut. identity change in expiration countdown uses:	□		
Direct init:	☑		
Identificator length:	12	bytes	
Verification method:	UCP		
Hash algorithm:	SHA-256		
Asymetric key algorithm:	RSA		
Asymetric key length:	2048	bits	
Signature algorithm:	SHA256withRSA		
Cipher transformation:	RSA/ECB/PKCS1PADDING		
Random string length:	24	bytes	
Key agreement protocol:	UCP		
Authentication key length:	8	bytes	
Replication key length:	24	bytes	
Init key agreement algorithm:	DH/AES/ECB/PKCS5Padding		
Session cipher transformation:	AES/CBC/PKCS5Padding		
Symmetric key length:	128	bits	
Hmac algorithm:	HmacSHA256		
Second authentication key length:	12	bytes	
Session key length:	16	bytes	
Signature encoding:	UTF-8		
Failure count (PEIG):	1	bytes	
Failure count (AIM):	1	bytes	
Vector length:	5	bytes	
Priority:	None		

Cyber identities validity

Cryptographic methods and their parameters

Security profile priority

Figure 6-1 Security profile – parameters

It is important for Security Managers to define parameters of cybernetic identity validity correctly so that they are in compliance with the local security requirements. The new defined cybernetic identity is valid for each new created identity in AIM from the moment the changes are saved and the profile is activated.

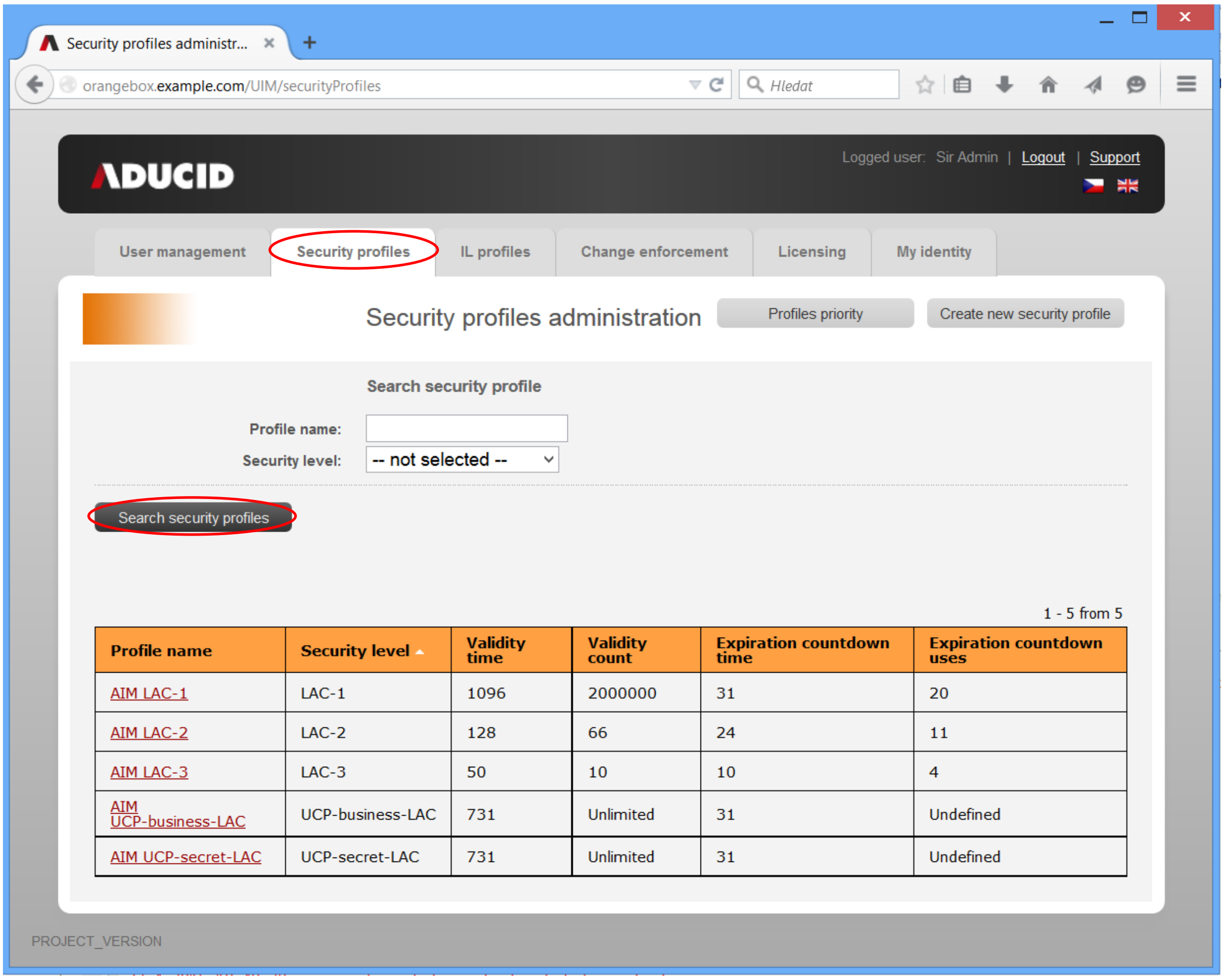
In this section, it is possible to change the cryptographic methods and parameters. A detailed explanation of the cryptographic methods and parameters is provided at a special training for Security Managers of ADUCID® systems. We strongly recommend leaving the security parameters unchanged, if the Security Manager has not participated in this training.

For commercial purposes, it is good to use the default AIM UCP-business-LAC profile or a higher variant AIM UCP-secret-LAC.

Priority can be set on every security profile. When use of current security profile is unsuccessful, security profile with lower priority is used, if defined.

6.1.2. Changes in existing security profile

Security profiles can be defined in the main UIM menu on the **Security profiles** tab.



Security profiles administr...
orangebox.example.com/UIM/securityProfiles
Hledat
ADUCID
Logged user: Sir Admin | Logout | Support
User management
Security profiles
IL profiles
Change enforcement
Licensing
My identity
Profiles priority
Create new security profile
PROJECT_VERSION

Security profiles administration

Search security profile

Profile name:

Security level: -- not selected --

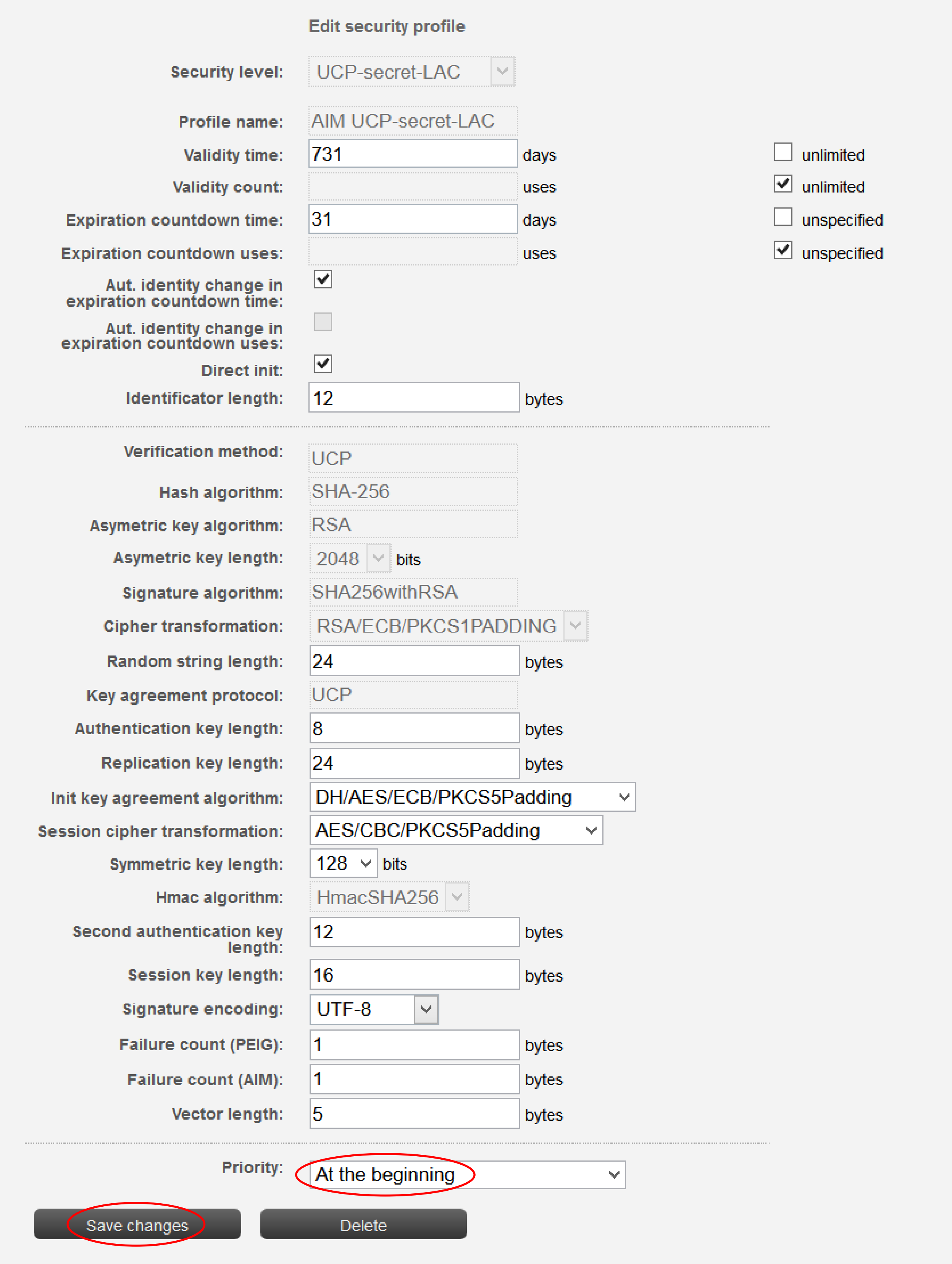
Search security profiles

1 - 5 from 5

Profile name	Security level	Validity time	Validity count	Expiration countdown time	Expiration countdown uses
AIM LAC-1	LAC-1	1096	2000000	31	20
AIM LAC-2	LAC-2	128	66	24	11
AIM LAC-3	LAC-3	50	10	10	4
AIM UCP-business-LAC	UCP-business-LAC	731	Unlimited	31	Undefined
AIM UCP-secret-LAC	UCP-secret-LAC	731	Unlimited	31	Undefined

Figure 6-2 Search security profiles

1. Click on the particular profile that you wish to change.
2. Make the required changes of the security profile and click **Save changes**. Be sure to set profile priority to the highest rank, i. e. “At the beginning”, if you want the changes to be valid for all new cybernetic identities immediately.



Edit security profile

Security level:	UCP-secret-LAC		
Profile name:	AIM UCP-secret-LAC		
Validity time:	731	days	□ unlimited
Validity count:		uses	☑ unlimited
Expiration countdown time:	31	days	□ unspecified
Expiration countdown uses:		uses	☑ unspecified
Aut. identity change in expiration countdown time:	☑		
Aut. identity change in expiration countdown uses:	□		
Direct init:	☑		
Identificator length:	12	bytes	
Verification method:	UCP		
Hash algorithm:	SHA-256		
Asymetric key algorithm:	RSA		
Asymetric key length:	2048	bits	
Signature algorithm:	SHA256withRSA		
Cipher transformation:	RSA/ECB/PKCS1PADDING		
Random string length:	24	bytes	
Key agreement protocol:	UCP		
Authentication key length:	8	bytes	
Replication key length:	24	bytes	
Init key agreement algorithm:	DH/AES/ECB/PKCS5Padding		
Session cipher transformation:	AES/CBC/PKCS5Padding		
Symmetric key length:	128	bits	
Hmac algorithm:	HmacSHA256		
Second authentication key length:	12	bytes	
Session key length:	16	bytes	
Signature encoding:	UTF-8		
Failure count (PEIG):	1	bytes	
Failure count (AIM):	1	bytes	
Vector length:	5	bytes	
Priority:	At the beginning		

Figure 6-3 Security profile—changing parameters

Legend:

Validity time—the maximum period of time (in days) for which the existing cybernetic identity is valid. Once this period is over, the identity must be renewed. If automatic identity renewal is switched on (see below), then this identity will be automatically renewed on the first log in in the expiration countdown time.

Validity count—the maximum number of uses of the existing cybernetic identity. The validity can be refreshed by renewing or changing the identity. The number of uses will be reset automatically.

Expiration countdown time—how long before the cybernetic identity expiry ADUCID® must warn the user. If the automatic renewal is switched on, there will be no warning and the identity will be renewed automatically.

Expiration countdown uses—how many times the identity can still be used before it expires and when the user must be warned.

Aut. identity change in expiration countdown time – automated identity renewal when the validity time period (in days) changes to the “expiration countdown time” period (the time before expiry equals or is shorter than the “expiration countdown time”).

Aut. identity change in expiration countdown uses – automated identity renewal when the number of identity uses equals (or is smaller than) the “expiration countdown uses”. The user’s identity will be automatically renewed on the first log in and the validity time and count will be reset.

Direct init – automated identity initialization if identity does not exist on the current PEIG® in the first use.

Identificator length – entropy of variable internal identificators of a cybernetic identity.

6.1.3. Identity renewal (options)

The identity status is indicated on PEIG® (or in UIM) by different colours. The meaning is the same as with traffic lights.

- **Green** —identity is valid and the user can go.
- **Orange** —expiry is near but the user can still go.
- **Red** —identity is invalid. The user cannot perform any operations.

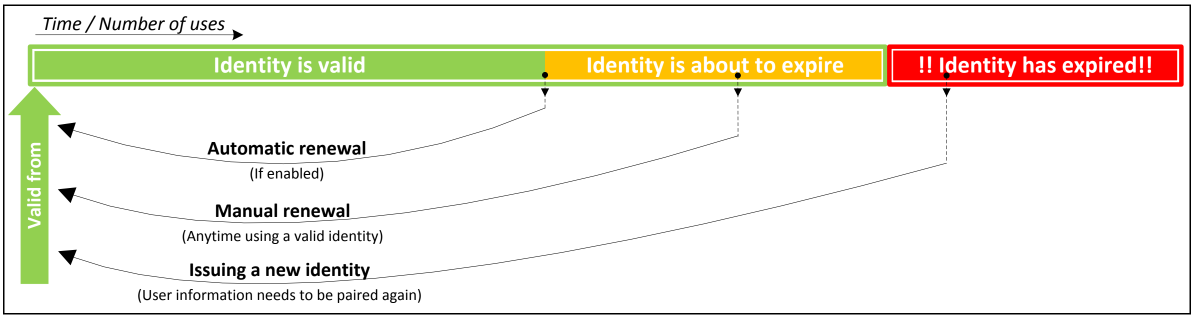

Time / Number of uses
Identity is valid
Identity is about to expire
!! Identity has expired!!
Valid from
Automatic renewal
(If enabled)
Manual renewal
(Anytime using a valid identity)
Issuing a new identity
(User information needs to be paired again)

Figure 6-4 Identity validity and renewal options

A user’s identity can be renewed in several different ways.

1. Automatically—no manual action is required from the user. \This option must be enabled by the UIM Security Manager.
2. Manually via UIM—at any time the user can click **Generate new identity** and **My identity**. This option can only be used if the identity is valid.
3. Manually via UIM after the identity has expired. The user is invited to create another identity. However, this action means that the original identity cannot be used any longer and the new identity must be paired with the profile of the user.

6.1.4. Creating your own security profile

If the profile that meets your requirements is not offered in the list of profiles, you can create your own. Proceed as follows:

1. Log in to UIM.
2. Click **Security profiles** and **Create new security profile**. The name of the profile can be empty—UIM will provide a list of all available security profiles.

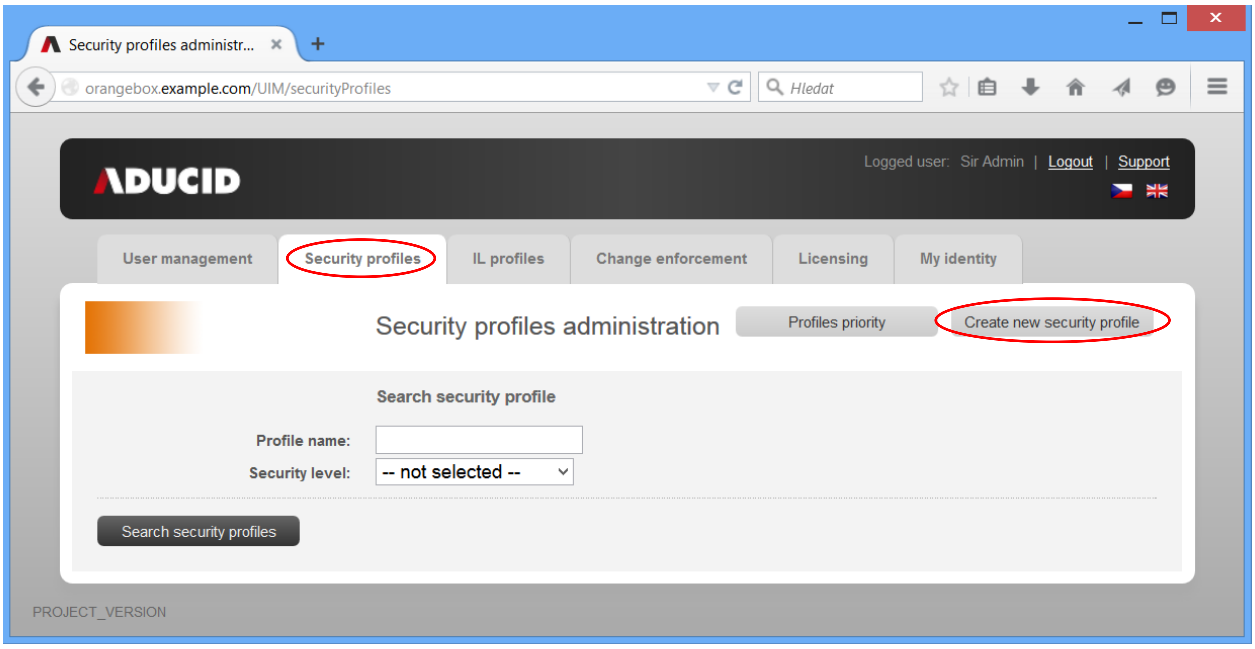


Figure 6-5 Create new security profile

3. Select a default security level to be used for the new security profile.

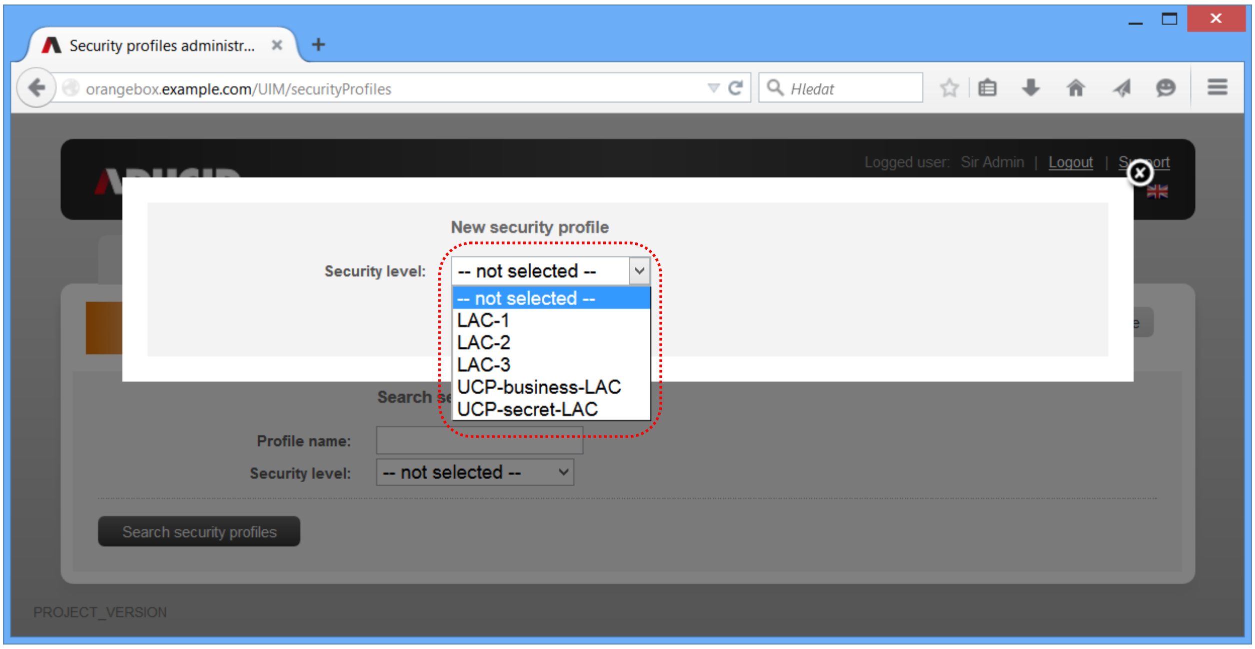
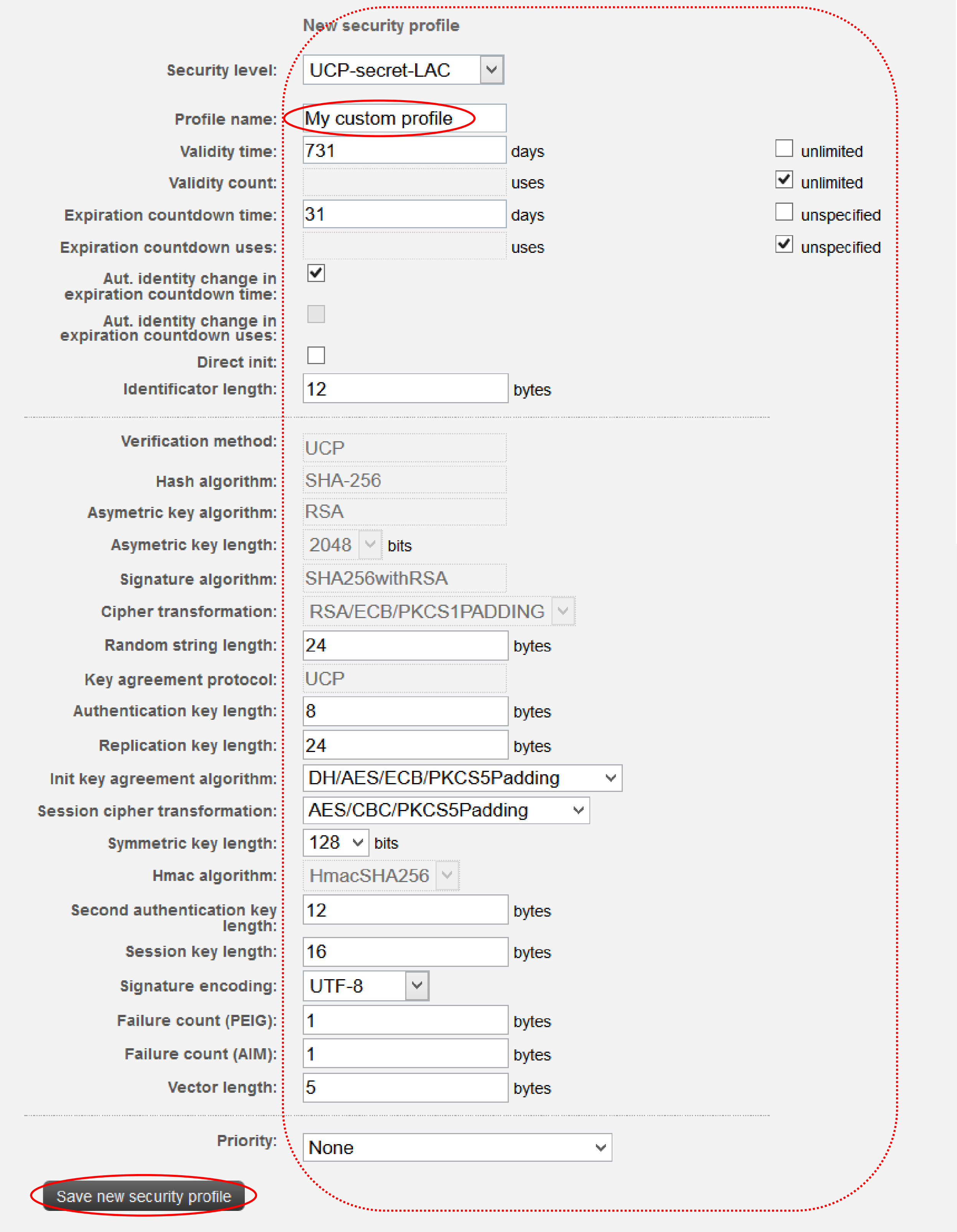


Figure 6-6 Select security level for new profile

4. Enter the new profile name, define the security profile parameters, and then click **Save new security profile**.



New security profile

Security level:	UCP-secret-LAC		
Profile name:	My custom profile		
Validity time:	731	days	☐ unlimited
Validity count:		uses	☑ unlimited
Expiration countdown time:	31	days	☐ unspecified
Expiration countdown uses:		uses	☑ unspecified
Aut. identity change in expiration countdown time:	☑		
Aut. identity change in expiration countdown uses:	☐		
Direct init:	☐		
Identificator length:	12	bytes	
Verification method:	UCP		
Hash algorithm:	SHA-256		
Asymetric key algorithm:	RSA		
Asymetric key length:	2048	bits	
Signature algorithm:	SHA256withRSA		
Cipher transformation:	RSA/ECB/PKCS1PADDING		
Random string length:	24	bytes	
Key agreement protocol:	UCP		
Authentication key length:	8	bytes	
Replication key length:	24	bytes	
Init key agreement algorithm:	DH/AES/ECB/PKCS5Padding		
Session cipher transformation:	AES/CBC/PKCS5Padding		
Symmetric key length:	128	bits	
Hmac algorithm:	HmacSHA256		
Second authentication key length:	12	bytes	
Session key length:	16	bytes	
Signature encoding:	UTF-8		
Failure count (PEIG):	1	bytes	
Failure count (AIM):	1	bytes	
Vector length:	5	bytes	
Priority:	None		

Figure 6-7 Define security profile parameters

5. Click OK to verify that the new profile was created successfully.

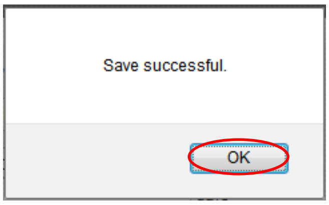

Save successful.

Figure 6-8 Profile successfully created

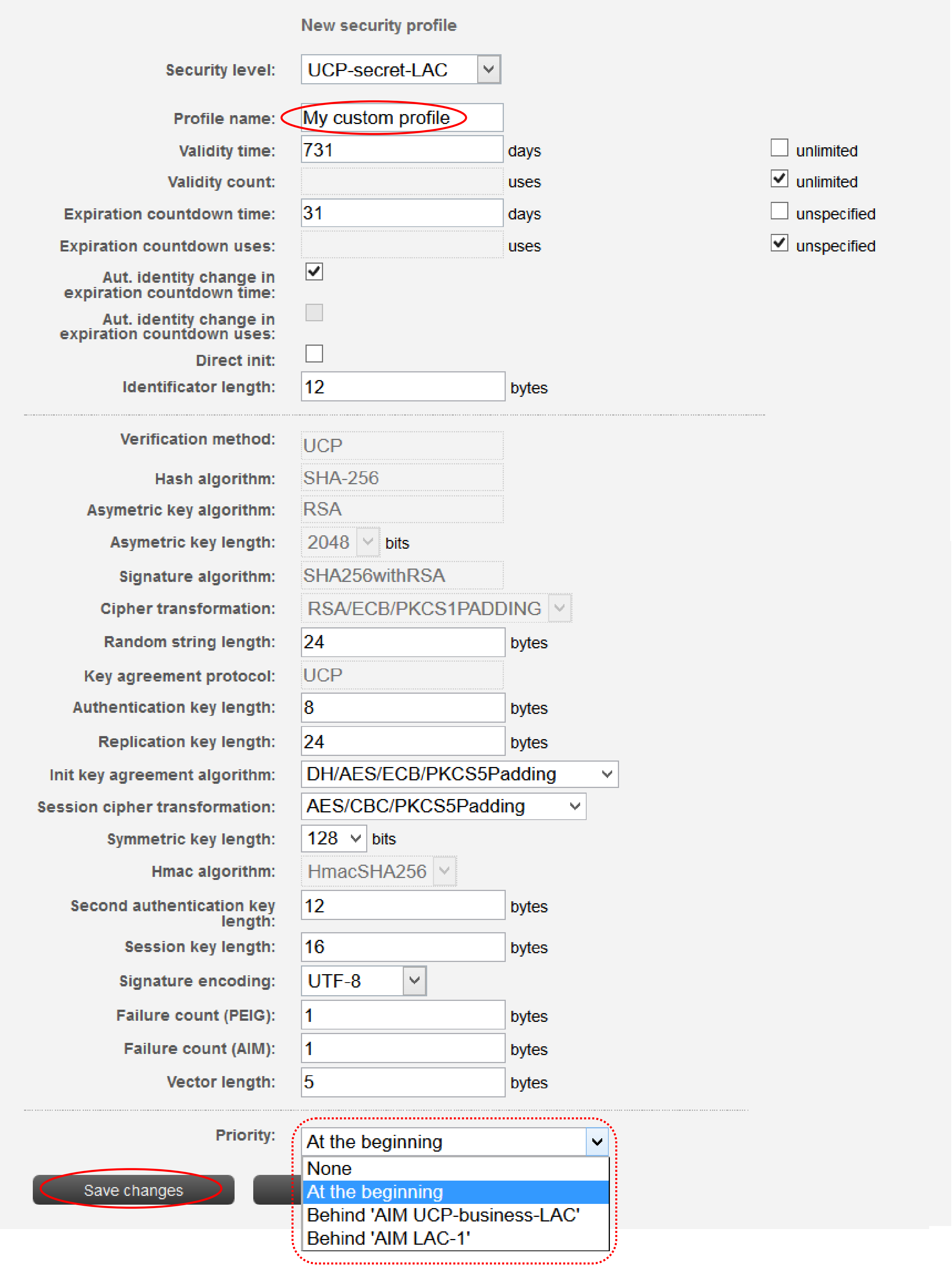
6. Do not forget to set priority to “At the beginning” value if you wish to apply it to all new identities.

6.1.5. Security profile priority

If you wish to change profile priority, proceed the same way that you do when you want to create or edit a profile.

1. Select **Security profiles**.
2. Click **Search security profiles**.
3. Click on the profile that you wish to modify.
4. Change profile **Priority** to requested value.

Priority marks security profile order. If profile with higher priority fails, profile with lower priority is used. Profile fails, if client and server are not able to communicate on current security profile. At first, profile with “At the beginning” priority value set is used.

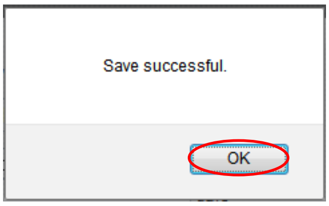


New security profile

Security level:	UCP-secret-LAC		
Profile name:	My custom profile		
Validity time:	731	days	☐ unlimited
Validity count:		uses	☑ unlimited
Expiration countdown time:	31	days	☐ unspecified
Expiration countdown uses:		uses	☑ unspecified
Aut. identity change in expiration countdown time:	☑		
Aut. identity change in expiration countdown uses:	☐		
Direct init:	☐		
Identificator length:	12	bytes	
Verification method:	UCP		
Hash algorithm:	SHA-256		
Asymetric key algorithm:	RSA		
Asymetric key length:	2048	bits	
Signature algorithm:	SHA256withRSA		
Cipher transformation:	RSA/ECB/PKCS1PADDING		
Random string length:	24	bytes	
Key agreement protocol:	UCP		
Authentication key length:	8	bytes	
Replication key length:	24	bytes	
Init key agreement algorithm:	DH/AES/ECB/PKCS5Padding		
Session cipher transformation:	AES/CBC/PKCS5Padding		
Symmetric key length:	128	bits	
Hmac algorithm:	HmacSHA256		
Second authentication key length:	12	bytes	
Session key length:	16	bytes	
Signature encoding:	UTF-8		
Failure count (PEIG):	1	bytes	
Failure count (AIM):	1	bytes	
Vector length:	5	bytes	
Priority:	At the beginning		

Figure 6-9 Security profile priority

After profile save, the following notification is displayed.

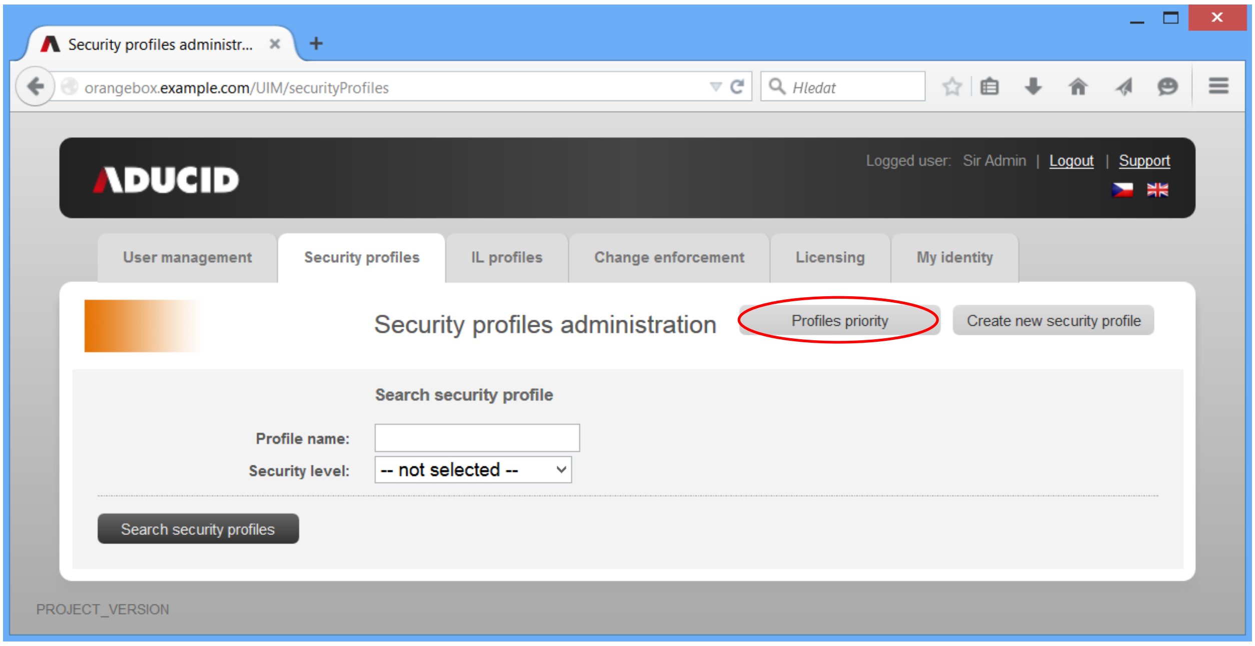


Save successful.

Figure 6-10 Notification

As soon as you change priority, all new operations with cybernetic identities will follow the rules of the new security profile priority sequence.

Current sequence of profiles priority can be shown by clicking on **Profiles priority** button on security profiles basic page.



Security profiles administration

Search security profile

Profile name:

Security level: -- not selected --

Figure 6-11 Profiles priority button

After click, image representing current security profile priority sequence, is shown. Profile with the highest priority is on the top. If client and server are not able to establish communication on security profile “My custom profile”, they try to use profile next in order, i. e. “AIM UCP-business-LAC”. This process is repeated while both sides, client and server, will not accept current security profile or there are not security profiles ordered in the priority sequence to use.

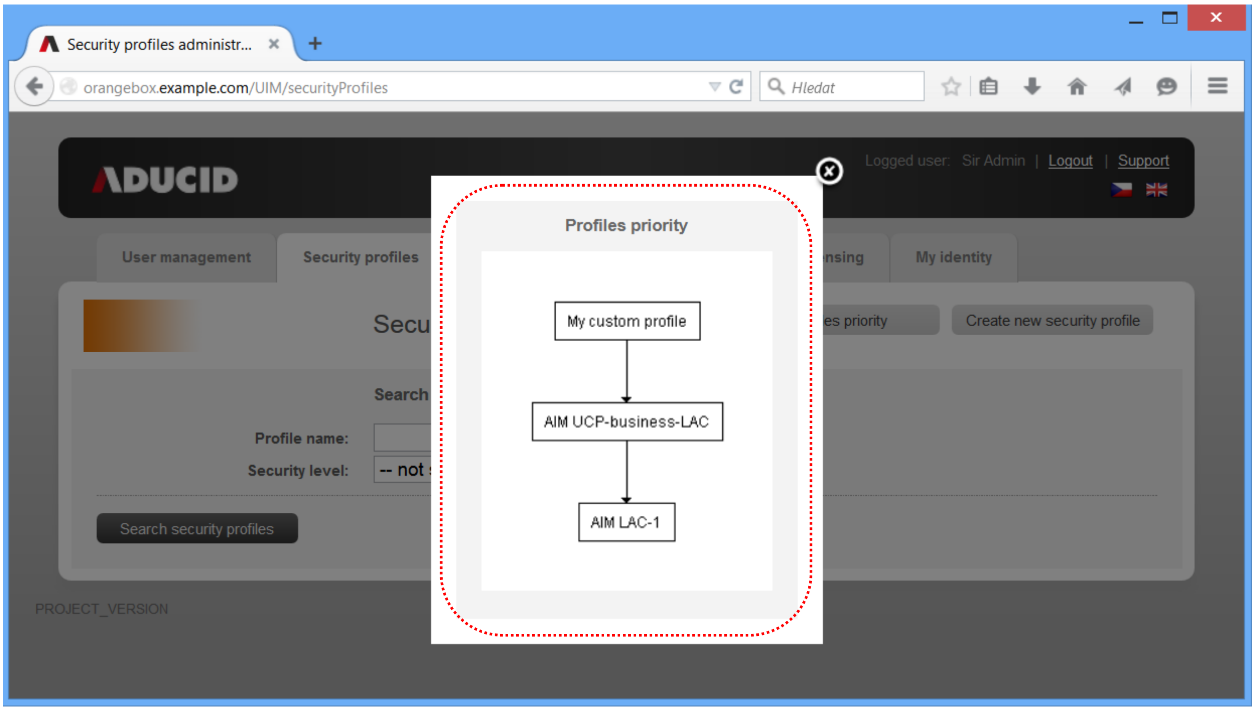


Figure 6-12 Current security profile priority sequence

6.2. Management of IL identificator parameters

The IL identificator is used for temporary shared identification of the user when the user's registration is being transferred from one provider to another. The following parameters can be managed by using **IL profiles** tab.

- Shared identity validity	[default one day]
- Identificator length	[default 8 bytes]

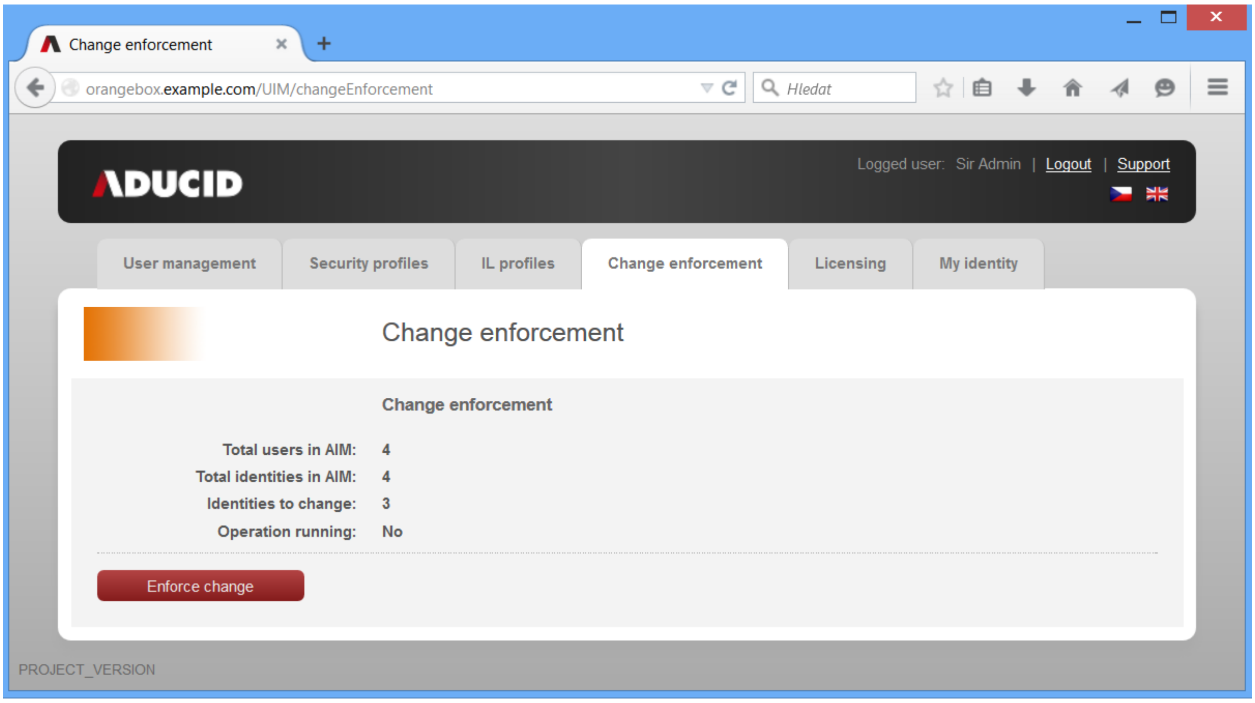
6.3. Enforcing security parameters changes

Enforced changes of security parameters are recommended.

- Quick change to new security parameters/methods
- Centrally enforced generating of shared asymmetric keys for individual identities

Everything is performed in a transparent way, and is not visible for the user, during normal operation. The change will be done only once for each PEIG$^{®}$ during the first log in.

Change enforcement can be done by clicking the **Change enforcement** tab, and then clicking **Enforce change**.



Change enforcement

Change enforcement

Total users in AIM:	4
Total identities in AIM:	4
Identities to change:	3
Operation running:	No

Figure 6-13 Enforcing identity parameters changes

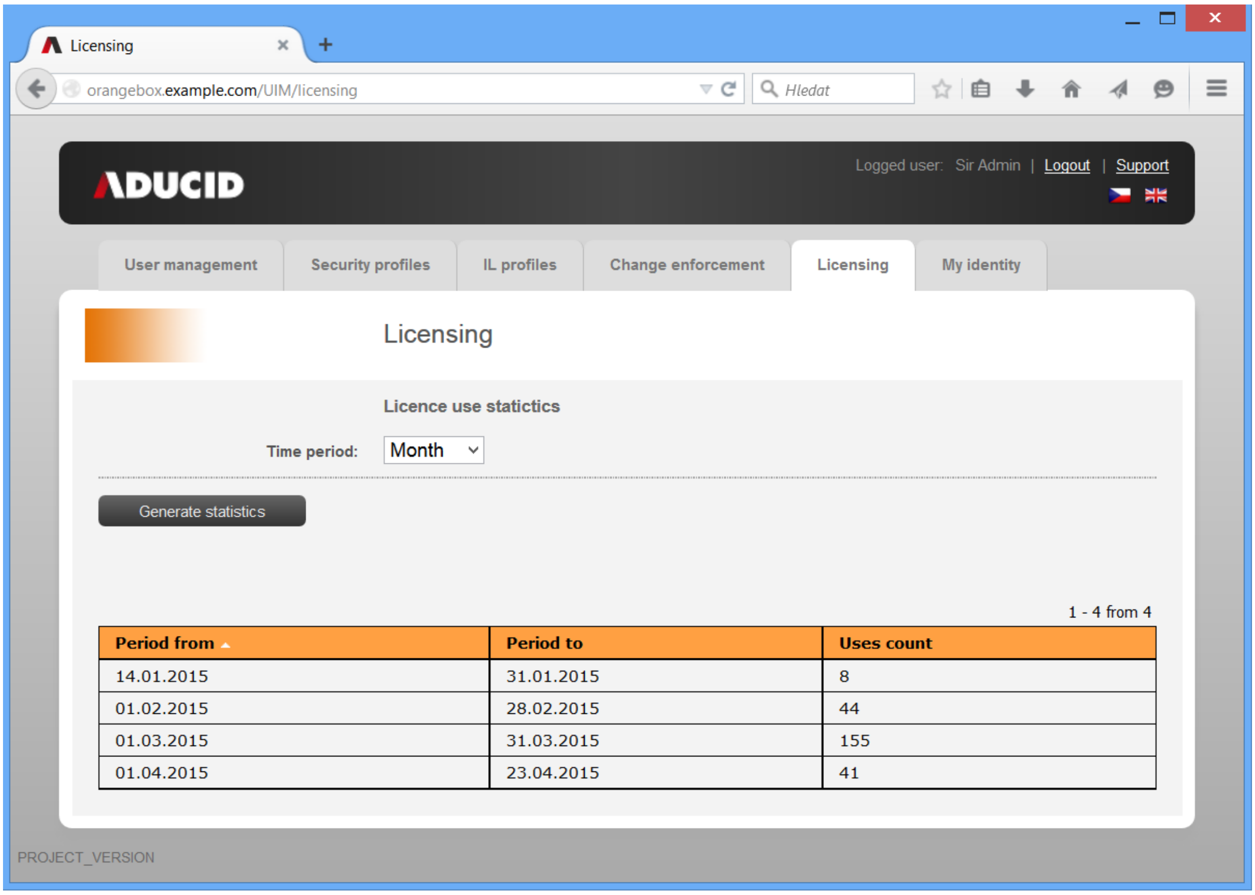
The Security Manager is able to monitor how many identities (PEIGs®) have been changed.

7. Used licences statistics monitoring

Security administrator can monitor used licences count in predefined time intervals. These time intervals are supported:

- Year
- Month
- Quarter

Statistics can be counted on “Licencing” tab clicking on “Generate statistics” button. Generated statistics example is shown on the figure below:



Licensing

Licence use statictics

Time period: Month

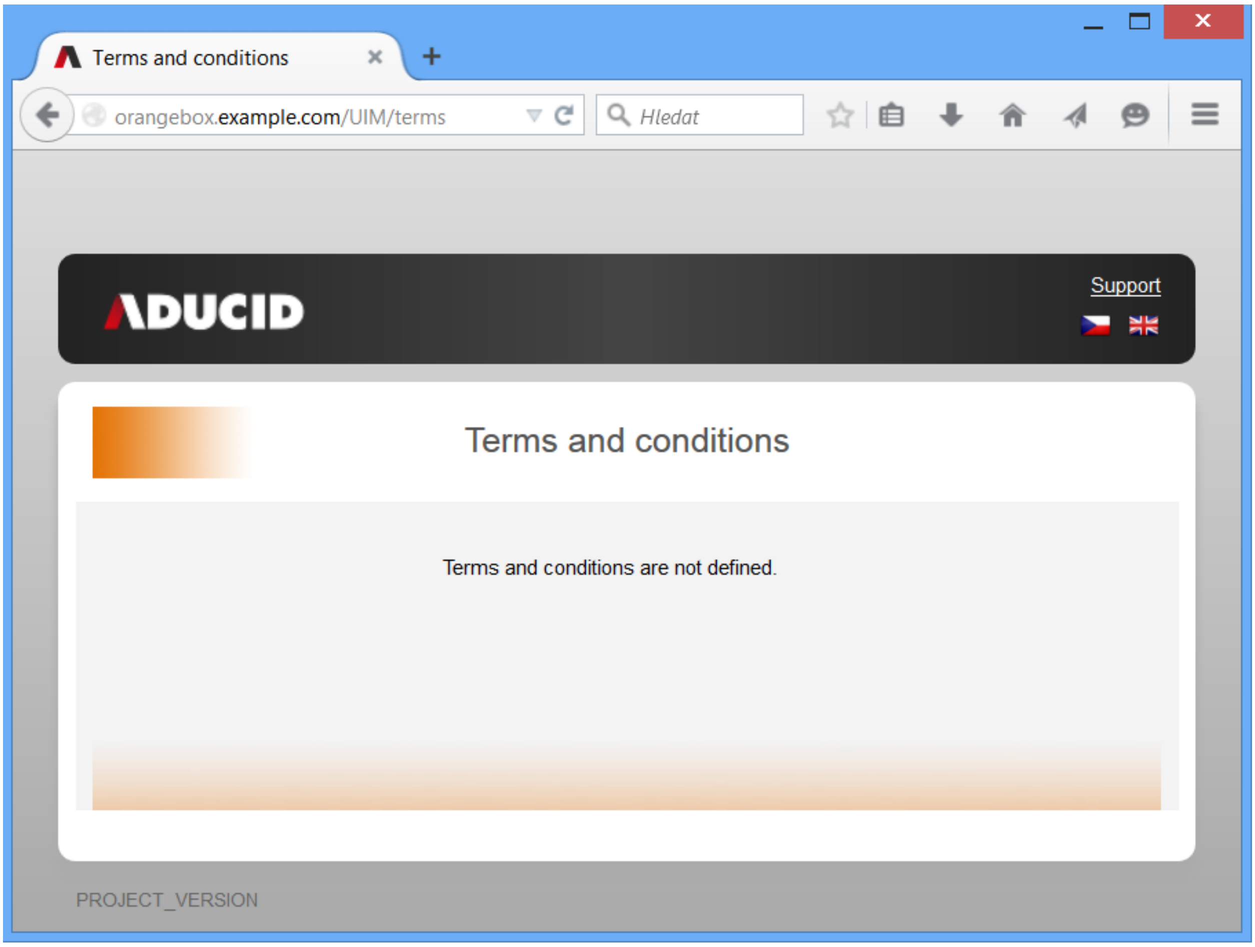
1 - 4 from 4

Period from ▲	Period to	Uses count
14.01.2015	31.01.2015	8
01.02.2015	28.02.2015	44
01.03.2015	31.03.2015	155
01.04.2015	23.04.2015	41

Figure 7-1 Used licences statistics

8. Defining terms and conditions

The application allows you to display your own terms and conditions. If the terms and conditions are not defined, the Terms and conditions page will read as follows:



Terms and conditions

Terms and conditions are not defined.

Figure 8-1 Terms and conditions not defined

You can create your own files with terms and conditions if you need to and you can integrate these files into the system. The procedure is as follows:

1. Prepare the following HTML files in the UTF-8 coding.
2. terms_cs.html—Czech version of the terms and conditions
3. terms_en.html—English version of the terms and conditions
4. The files belong to ADUCID Server Kit (folder `/var/lib/tomcat6/webapps/UIM/WEB-INF/pages`). However, this folder is not persistent and will be deleted during updates. We strongly recommend creating the folder `/etc/tomcat6/customization`. Move the files to this folder. Then create a symbolic link from `WEB-INF/pages` to `/etc/tomcat6/customization`. A possible procedure is suggested below.

```
mkdir /etc/tomcat6/customization
# copy your files terms_* to /etc/tomcat6/customization
cp ~/terms_* /etc/tomcat6/customization/
chmod 644 /etc/tomcat6/customization/terms_*
cd /var/lib/tomcat6/webapps/UIM/WEB-INF/pages
rm -f terms_cs.html terms_en.html
ln -s /etc/tomcat6/customization/terms_cs.html
ln -s /etc/tomcat6/customization/terms_en.html
```

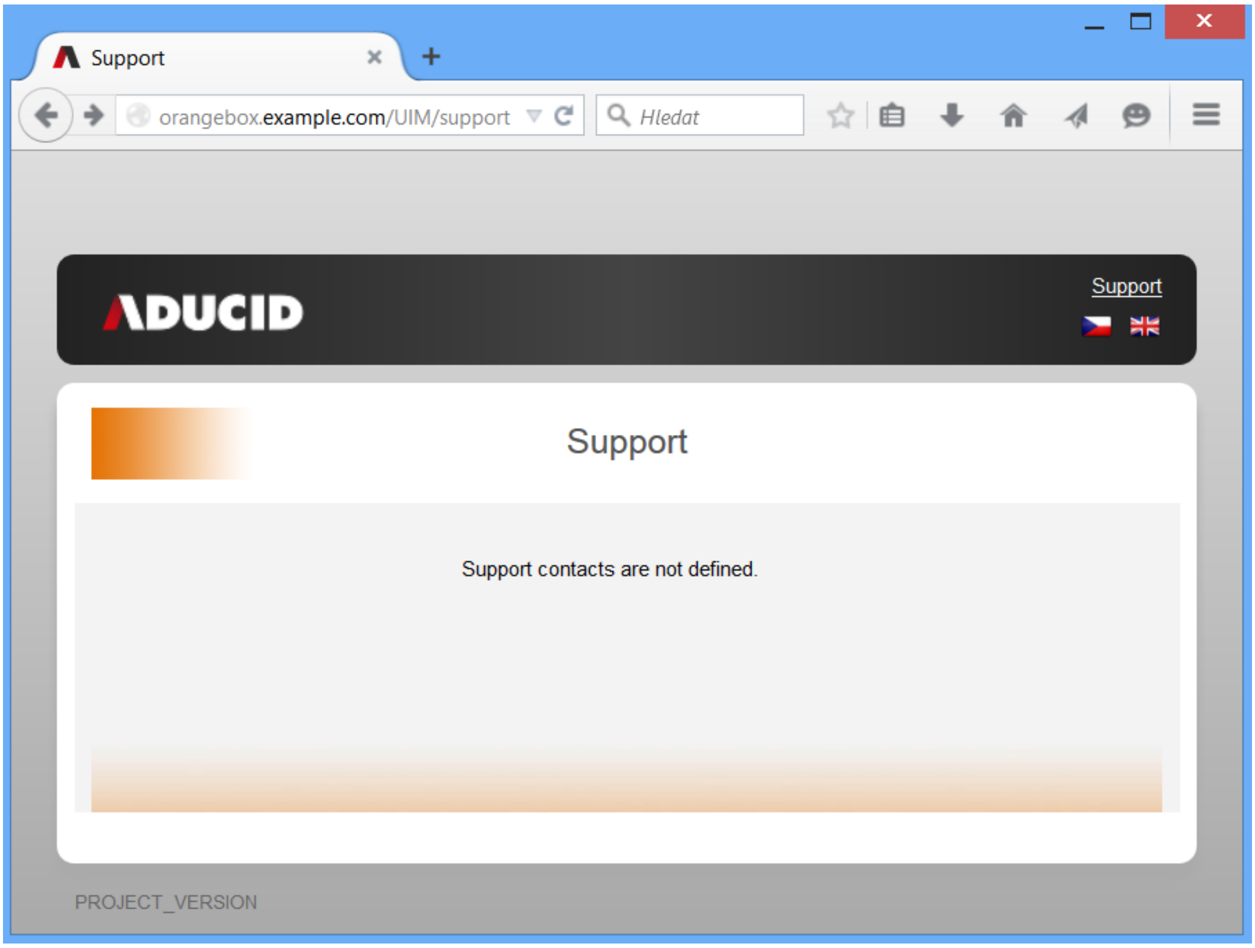
It is necessary to renew the symbolic links after an update, but the changes themselves will not be lost.

5. Restart the Apache Tomcat application server

Your terms and conditions will now be automatically loaded to the body of the Terms and conditions page.

9. Support contacts

The application allows you to display your own support contacts. If the contacts are not defined, the contact page reads as follows:



Support contacts are not defined.

Figure 9-1 Support contacts not defined

You can create your own files with support contacts and you can integrate these files into the system. The procedure is as follows:

1. Prepare the following HTML files in the UTF-8 coding with your support contacts:
   a. terms_cs.html—Czech version of support contacts
   b. terms_en.html—English version of support contacts
2. The files belong to ADUCID Server Kit (folder `/var/lib/tomcat6/webapps/UIM/WEB-INF/pages`). However, this folder is not persistent and will be deleted during updates. We strongly recommend creating a folder `/etc/tomcat6/customization`. Move the files to this folder. Then create a symbolic link from `WEB-INF/pages` to `/etc/tomcat6/customization`.

   It will be necessary to renew the symbolic links after an update, but the changes themselves will not be lost.

3. Restart the Apache Tomcat application server

Your support contacts will now be automatically loaded to the body of the support contacts page.

10. References

[1] *ADUCID® Architecture*

[2] *ADUCID® Integration Guide*

[3] *ADUCID Server Kit – Instalation Guide*

[4] *ADUCID Server Kit – Administration Guide*

[5] *UIM – User Guide*

[6] *UIM – Administration Guide*