

BRNO UNIVERSITY OF TECHNOLOGY

DIPLOMA THESIS

Cryptography and Privacy Protection

INSTALLATION AND USER GUIDE

Author:

Bc. Ondrej MALÍK



May 24th, 2021

Contents

1	Installation guide	3
1.1	Node.js	3
1.1.1	Installing Node.js using NodeSource repository	3
1.1.2	Installing Node.js using Ubuntu official repository	3
1.2	Web application	4
2	User guide	6
2.1	Issuer' app	6
2.1.1	Card personalization	6
2.1.2	Assigning attributes	7
2.1.3	Managing keys	7
2.1.4	Smart-card readers	8
2.1.5	Reseting application	8
2.2	Revocation authority's app	9
2.2.1	Revocation handler	9
2.2.2	Managing files	9
2.2.3	List of verifiers	10
2.2.4	Revoking user	10
2.2.5	Reseting application	10
2.3	Verifier's app	10
2.3.1	Managing keys	12
2.3.2	Access credentials	13
2.3.3	Epoch management	14
2.3.4	Reseting application	14
2.3.5	Access logs	14
3	Proof of concept	16
3.1	Server preparation	16
3.2	Client preparation	16
3.3	Assigning attributes to card	17
3.3.1	Personalization of the card	18
3.3.2	Assigning revocation handler	19
3.3.3	Permitting verifier	19
3.3.4	Managing the keys	20
3.3.5	Assigning attributes	20
3.4	Verifying attributes	21
3.4.1	Integrating verifier to RKVAC	22
3.4.2	Preparing access credentials	22

3.4.3	Connecting to RA	23
3.5	Revoking user	24

1 Installation guide

This chapter serves as a guide for installing web applications to the system. Recommended operating system for running applications is Ubuntu Server LTS. The installation process is same for all three applications except the debugging of RKVAC application.

1.1 Node.js

Web applications are build on JavaScript back-end framework Node.js. Node.js is a JavaScript runtime built on Chrome's V8 JavaScript engine. The best way to install Node.js and all application dependencies is via Node Package Manager (NPM). There are multiple ways to install NPM to your system. Two easiest ways are included in this guide.

Important: Node.js version **16.x** is not supported. It is recommended to install the latest release of version **15.x** as shown in this guide.

1.1.1 Installing Node.js using NodeSource repository

1. Connect to your server's terminal and write these commands:

```
# Using Ubuntu
$ curl -fsSL https://deb.nodesource.com/setup_15.x \
$ | sudo -E bash -
$ sudo apt-get install -y nodejs
//
# Using Debian, as root
$ curl -fsSL https://deb.nodesource.com/setup_15.x \
$ | bash -
$ apt-get install -y nodejs
```

2. Following commands should return similar output:

```
$ node -v
v15.13.0
$ npm -v
7.7.6
```

1.1.2 Installing Node.js using Ubuntu official repository

1. Connect to your server's terminal and write these commands:

```
$ sudo apt-get update
$ sudo apt-get install nodejs
$ sudo apt-get install npm
```

2. Following commands should return similar output:

```
$ node -v
v15.13.0
$ npm -v
7.7.6
```

After following these instructions Node.js with Node Package Manager should be installed in the system.

1.2 Web application

After installing Node.js, download the web application to the server. Following steps shows the installation process for one of the web applications.

1. Download the web application to the server.
2. Install all dependencies for RKVAC application.
3. Follow the instructions for debugging RKVAC application with these specialties:
 - there is no need to patch `pcsc` library, due to the remote communication with the card,
 - build option for remote communication with ID card should be set to:
`-DRKVAC_PROTOCOL_REMOTE`
 - TCP port for communication between RKVAC and web application needs to be set in the header file accordingly to web application:
 - Verifier' application – port 5000
 - RA's application – port 5001
 - Issuer's application – port 5002

The port can be specified before debugging in the header file, see Listing 1.1

4. Copy the RKVAC executable to the parent folder of web application.
 - The executable should be named `rkvac-protocol-multos-1.0.0`.
5. Run application using command:

```
$ npm run serverstart
```

6. Connect to web server using address `https://<server-address>:<port>/` where:
 - **server-address** is IP address or domain name of the machine where the web app is running
 - **port** is web port of https server:
 - Verifier' application – port 8443
 - RA's application – port 9443
 - Issuer's application – port 10443

Listing 1.1: rkvac-server/service/config/network-config.h

```
#ifndef __RKVAC_PROTOCOL_SERVICE_NETWORK_CONFIG_H_
#define __RKVAC_PROTOCOL_SERVICE_NETWORK_CONFIG_H_

#ifdef __cplusplus
extern "C"
{
#endif

#define SRV_IPV4_ADDRESS "127.0.0.1"
#define SRV_PORT <PORT>

#define MAX_TRANSMIT 4096

#define SA struct sockaddr

#ifdef __cplusplus
}
#endif

#endif /* __RKVAC_PROTOCOL_SERVICE_NETWORK_CONFIG_H_ */
```

2 User guide

This chapter is divided in three sections, where each contains user manual for one of three applications created in the diploma thesis. For all functions to work properly, all steps stated in chapter 1 needs to be implemented.

2.1 Issuer' app

After connecting to the https server on address `https://<server-address>:10443/`, you will be automatically redirected to login page. Default logging-in credentials:

- username – **admin**
- password – **Vut2021**

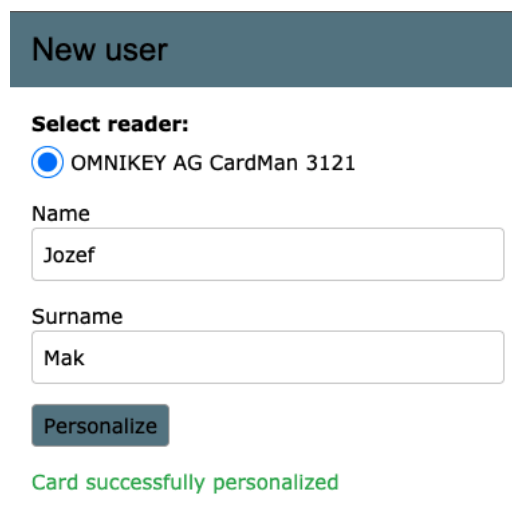
After log-in, you will be redirected to the home page.

2.1.1 Card personalization

Functions for card personalization are available on the „Users“ page. Navigation to this page is possible using both menu bar or the „Users“ panel on the home page.

On the left side of the „Users“ page a list of all personalized ID cards is placed. Each ID has a **name**, **surname** and a **ID number**, which is assigned automatically. The user list can be refreshed using a refresh button or by refreshing the web page.

For personalization of a new card connected to your PC, use the panel „New user“ placed on the right side of the page. Choose the **smart-card reader** you want to use and enter card user's **name** and **surname**. After clicking on the button „Register“ the personalization process is started. At the end of the process the success or error message is shown on the bottom of the panel (see Fig. 2.1). After successful personalization of a smart-card, the new



New user

Select reader:

☒ OMNIKEY AG CardMan 3121

Name

Jozef

Surname

Mak

Personalize

Card successfully personalized

Fig. 2.1: Card personalization

entry is added to user list. For further usage a revocation handler needs to be assigned to the card (see section 2.2.1).

2.1.2 Assigning attributes

Functions for assigning attributes to smart-card are available on the „credentials“ page. Navigation to this page is possible using both menu bar or the „Credentials“ panel on the home page. For assigning attributes to the given smart-card, the card needs to have a **revocation handler** assigned (see section 2.2.1), and the **public key of revocation authority** needs to be uploaded to the issuer's application (see 2.1.3).

Attributes are assigned to the card via credentials files. New credentials file can be created using left panel „New credentials“. Following 4 types of credentials are available:

- **EID,**
- **Ticket,**
- **Employee Card,**
- **Own-defined.**

After choosing the type of credentials, appropriate attributes can be defined. In case of own-defined credentials as much as 9 attributes can be defined. After entering all attributes and clicking on „Assign credentials“ button, the new credentials file containing defined attributes is created and assigned to smart-card in chosen smart-card reader (see Fig. 2.2). In the table on the left side of the page all credentials files are listed. Using appropriate icons, credentials files can be deleted, viewed and re-assigned to connected card.

2.1.3 Managing keys

For proper working of RKVAC system, the **revocation authority's public key** needs to be uploaded to issuer's application. This can be done using panel „Tools“, available on the home page of application. After choosing revocation authority's public key file from user's file system, and clicking on the „Upload“ button, the file is uploaded to the system (for obtaining the key as a revocation authority, see section 2.2.2). In case of migrating RA's system, the public key can be deleted and replaced with a new one. For proper working of the application, the file containing RA's public key needs to be named **ra_pk.dat**.

Functions for managing **issuer's private key** are also available through panel „Tools“. This key is automatically generated during the first assigning of attributes to the card. Using the button „Download“, the key can be downloaded for further usage. In case of implementing issuer's entity from other system, the private key can be uploaded from user's file system. If the key is imported, it is not generated during the first assigning of attributes. For proper working of the application, the file containing issuer's private key needs to be named **ie_sk.dat**.

New credentials

EID

Ticket

Employee's card

Own

Select reader:

☒

 OMNIKEY AG CardMan 3121

Title

JozefMak

Number of attributes

4

Attribute1

Jozef Mak

Attribute2

Male

Attribute3

db-admin

Attribute4

vut-teacher

Assign credentials

Credentials successfully created and assigned

Fig. 2.2: Assigning attributes

2.1.4 Smart-card readers

At the home page of the application on the panel „Smart-card Readers“, all smart-card readers plugged in the user’s computer are listed. After clicking on the particular reader, the card inserted in it is contacted with SELECT AID message. In case of ACK response, the card is marked as properly working.

2.1.5 Reseting application

For resetting the application to its default state, the button on the panel „Application’s reset“ can be used. Note that this will remove all RKVAC files (with exception of RKVAC executable) and any previous actions will be lost.

2.2 Revocation authority's app

After connecting to the https server on address `https://<server-address>:9443/`, you will be automatically redirected to login page. Default log-in credentials:

- username – **admin**
- password – **Vut2021**

After logging-in, you will be redirected to the home page. In case of first usage of the application, you will be prompted to initialize the RKVAC application. After clicking on the „Initialize“ button, the appropriate folders are created on the server.

2.2.1 Revocation handler

Revocation handlers can be assigned using the panel „Assigning revocation handler“. All smart-card readers plugged in user's computer are listed in this panel. After selecting one, the card inserted in it is contacted with SELECT AID message. In case of ACK response, the card is marked as properly working. By using the „Assign“ button, the assigning process is started. On the end of the process, the appropriate message is showed on the bottom of the panel (see Fig. 2.3).

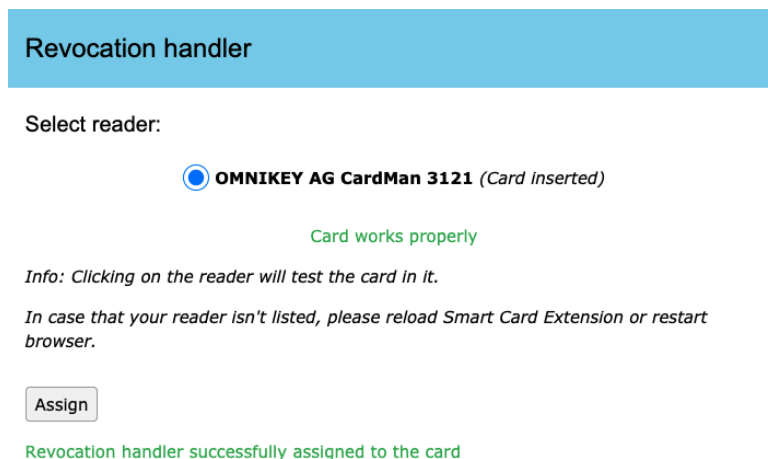


Fig. 2.3: Assigning revocation handler

2.2.2 Managing files

Revocation authority's **private** and **public files** can be managed using functions on the „Revocation authority's files“ panel. All these files are generated during the first usage of „Assigning revocation handler“ function. Using „Download“ buttons, files are downloaded for further usage. In case of implementing revocation authority from other system, these files can be uploaded from the local file system. Files, that are uploaded before the first usage, won't be automatically generated.

2.2.3 List of verifiers

In order to change a epoch, verifiers are connecting to revocation authority's application. RA activate their epoch, update the user blacklist and send it back to verifiers. By default revocation authority accepts connections only from IP addresses listed in „Permitted verifiers“. Functions for managing this list are placed in „Verifiers“ page, accessible through top menu bar.

Verifier's IP address can be added to the list, and then deleted. Application uses only IPv4 addresses.

2.2.4 Revoking user

Revocation of the users from the RKVAC system, can be accomplished using functions on the „User's revocation“ panel. For a successful revocation, following information needs to be filled in the form:

- **User's ID or pseudonym C** – user's ID can be provided by an issuer (see Fig. 2.1.1). Pseudonym C is available in the access logs of the verifier's app (see 2.3.5).
- **Epoch number** – only if revoking pseudonym C . The number of the current verifier's epoch can be found in the verifier's app (see 2.3.5).
- **Verifier's server address** – IP address or domain name of the verifier's server. In case more verifiers, addresses needs to be separated with ,.

After providing all necessary information and starting the process by clicking on the „Revoke“ button, the blacklist for the given epoch is updated and sent to the verifier. On the verifier's side, the blacklist is automatically rewritten based on the received one, and the user is revoked from the system (see Fig. 2.4).

2.2.5 Resetting application

For resetting the application to its default state, the button on the panel „Application's reset“ can be used. Note that this will remove all RKVAC files (with exception of RKVAC executable) and any previous actions will be lost.

2.3 Verifier's app

The web application that implements the verifier's site of RKVAC system, created in this diploma thesis, consists of two parts. This manual will provide steps for using the main part, which is the authentication module based on RKVAC system. The second part is the database of university classes, teachers and departments, which is just a example of a web service, that can be protected by the authentication module.

Revocation of a user

User's identifier:

User's pseudonym C:

Only one of pair identifier-pseudonym can be specified.

Epoch number:

Epoch number is required only if revoking pseudonym.

Verifier's address:

In case of multiple verifiers separate addresses with commas

User successfully revoked from system

Fig. 2.4: Revocation of a user

After connecting to the https server on address `https://<server-address>:8443/`, you will be automatically redirected to a login page. The login page offers two kinds of authentication:

1. **RKVAC authentication** – authentication using RKVAC attributes is executed in two steps:

- (a) **Selecting the smart-card reader** – from the list of all smart-card reader, plugged in the user's machine. When a smart-card reader is selected, the card in it is tested with SELECT AID message. In case of ACK answer, the smart-card is marked as properly working.
- (b) **Choosing the user-role** – after selecting the smart-card reader, user needs to select the user-role, with which he wants to authenticate towards the application.

Following three user-roles are available – **Admin**, **Teacher**, **Student**.

When a user-role is selected, the authentication process automatically starts (see Fig. 2.5). User's smart-card is contacted with challenge to provide the proof of holding the required attributes. In case of successful verification of the proof, user is logged in, and is authorized for actions based on the selected user-role. In case of authentication failure the appropriate message is shown.

2. **Local authentication** – At the default state, the application is not ready for RKVAC authentication. For administration purposes the local authentication is placed in the bottom of the login page. Default log-in credentials:


- username – **admin**

- password – **Vut2021**

After logging-in, you will be redirected to the home page.

Login

Select a reader:


 **OMNIKEY AG CardMan 3121** (Card inserted)

Card works properly

*Info: Clicking on the reader will test the card in it.
In case that your reader isn't listed, please reload Smart Card Extension or restart browser.*

Log in as:

Admin Teacher Student



Local authentication

Fig. 2.5: RKVAC authentication

Whole RKVAC administration is based at the „Setup“ page, which is available through the left-side panel. Along with „Access logs“ page (see 2.3.5), only administrators are permitted to access this page.

In case of first usage of the application, you will be prompted to initialize the RKVAC application. After clicking on the „Initialize“ button, the appropriate folders are created on the server.

2.3.1 Managing keys

For proper working of RKVAC system, verifier's application needs to have access to following files:

- issuer's private key
- revocation authority's public key
- revocation authority's public parameters

All these files can be uploaded via the „RKVAC keys“ panel. In case of system migration, all files can be later deleted and replaced with other ones.

2.3.2 Access credentials

Functions for administration of access credentials are placed in „Access credentials“ panel. In the initiate state of the app, none of the access credentials are created. As an admin we need to prepare credentials for each user-role, that will have an access to the system. In the credentials we define attributes, that we want to verify, and their position. The current state of the access credentials is displayed in the table (see Fig. 2.6). If the access credentials for one of the user-roles are created, they are marked as **ready**, and there is a possibility to delete them. Details of the credentials can be displayed via „info“ icon, placed next to the user-role name.

Access credentials		
Role	State	Action
Admin ⓘ	ready	Delete
Teacher ⓘ	ready	Delete
Student ⓘ	ready	Delete

Fig. 2.6: Access credentials table

Creation of a new access credentials is performed in these steps:

1. **Choosing user-role** – each role is available for selecting, only if it doesn't have any other credentials prepared.
2. **Selecting attributes count** – number of attributes in the credentials needs to be the same, as the number of attributes in the credentials, with which the users of RKVAC system would request to log-in to the application.
3. **Defining attributes** – only the attributes that will be used for logging-in needs to be declared. Other field can be left blank. Attributes needs to be set up on the exact same position, as are the same attributes in the user's credentials.
4. **Required attributes position** – parameter specifies the position of attributes, that will be requested during the authentication process.

If the user has assigned the credentials with these attributes:

- attribute 1: **Jozef Mak**
- attribute 2: **Male**
- attribute 3: **db-admin**
- attribute 4: **vut-teacher**

then the credentials that would provide him admin access to this database could have this structure:

- attribute 1:

- attribute 2:
- attribute 3: **db-admin**
- attribute 4: **vut-teacher**
- Required attributes position: **3,4**

With this example set as a admin credentials, any user that provides prove of holding attributes **db-admin** and **vut-teacher** in the positions **3** and **4** in his credentials, would be logged-in with administrator access.

2.3.3 Epoch management

Functions for epoch management are placed in the panel „Epoch settings“. At the top of this panel, a current epoch number is stated. After using the button „Switch now“ a new epoch is generated, and sent to the revocation authority for activation.

For proper working of the epoch switching function, an **address of revocation authority's server** needs to be set up. After entering the IP address or domain name of the server, it is saved in the back-end of the application, and the epoch switching function is enabled.

At the bottom of the „Epoch settings“ panel, function for scheduling a regular epoch switching is available. Time expression needs to be entered in the **crontab format**. The expression consists of 5 fields separated by space. Each field defines different time unit of the scheduling job – „<minute> <hour> <day(month)> <month> <day(week)> “, where the character * defines the value „each“. Practically an expression `0 0 * * *` would schedule the task to be run each day at 0:00 every month. Another example is an expression `45 * * * *`, which would schedule the task to be run every hour at 45th minute. Admin can use the crontab help, available at following link <https://crontab.guru>.

2.3.4 Reseting application

For resetting the application to its default state, the button on the panel „Application's reset“ can be used. Note that this will remove all RKVAC files (with exception of RKVAC executable) and any previous actions will be lost.

2.3.5 Access logs

User with administrator privileges can access the web page „Access logs“, available through left-side panel. At this page, the list of 50 most recent access logs are available. Each log consists of:

- **timestamp**,
- **epoch number**,
- **pseudonym C**,
- **result** – access **ALLOWED** or **DENIED**.

User's pseudonym C and epoch number, can be sent to the revocation authority in order to revoke the user from RKVAC system.

Logs are displayed in reverse order – the most recent are on the top of the list. The list is limited to contain the last 50 records. Older logs can be found directly on the server in the file `./data/Verifier/ve_requests.log`.

3 Proof of concept

In this chapter a full proof of concept is described. Following these steps, you will test the majority of the functions of web applications, created in this diploma thesis. All steps described in this chapter are for demonstration purpose. For easier start, it is recommended to use prepared virtual machines for both server and client appliances, that are saved in the shared folder on Google Drive. The folder is available for all members of the group „Brno University of Technology“ and it contains two virtual machines:

- **RKVAC Server** – Ubuntu Server 20.04 LTS. This appliance serves as a server, on which all three web applications are running. The following structure is prepared on the machine:
 - all dependencies of RKVAC application are installed,
 - the RKVAC application for each web application is compiled and ready,
 - all dependencies from „Installation guide“ are installed,
 - each RKVAC entity has its own user account, created for simulation of independent environments,
 - in /home folder of each user, there is a directory named `rkvac-<entity>`, which contains cloned GitHub repository of the particular application.
- **RKVAC Client** – Windows Desktop 10. This appliance serves as a client for all web applications. The only thing that is prepared in this appliance is installed Google Chrome with the Smart Card Extension.

3.1 Server preparation

In this section you will prepare the server. At the end you will have all applications running on the virtual machine.

1. Download the virtual machine **rkvac-server** from the link in the introduction of this chapter.
2. Open the virtual machine in VMware Workstation.
3. Before starting the machine, make sure that the network adapter is set in the mode **bridged** – see Fig. 3.1. In this mode the virtual machine will be connected directly to your local network.
4. Start the virtual machine.

After booting the virtual machine you should see on login page addresses of web applications (see Fig. 3.2). All application should be running on specified port on IP address of the machine.

3.2 Client preparation

Client is a Windows Desktop virtual machine, that have installed Google Chrome with Smart Card Extension. In these few steps you will prepare the client's machine, so that you will be

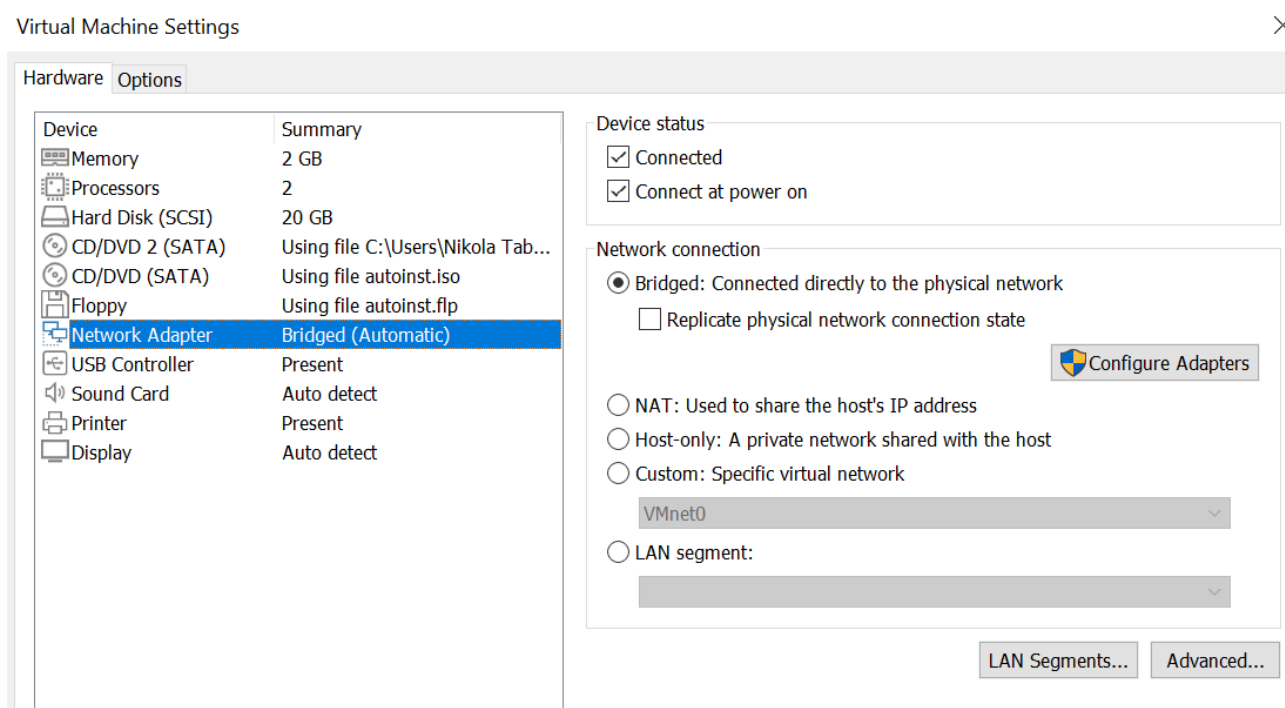


Fig. 3.1: Network adapter needs to be set to **bridged**

able to use RKVAC functions in the application.

1. Download virtual machine rkvac-client
2. Make sure that the network adapter of the virtual machine is set to „bridged“ (see Fig. 3.1) – we won't need client's IP address in order to use web applications.
3. Start the virtual machine.
4. Log in using credentials:
 - username – **admin**
 - password – **Vut2021**
5. Connect a smart card reader with appropriate card to your computer.
6. Connect the reader to the virtual machine – this is available through „Virtual Machine Settings -> USB Controller“
7. Start Google Chrome

3.3 Assigning attributes to card

In this section the process of integration of the card to the system is described. In order to fully integrate the card you need to:

- **personalize the card,**
- **assign revocation handler to the card,**
- **import revocation authority' key to the issuer,**
- **assign attributes to the card.**

```
WELCOME TO RKVAC SERVER
All application should be running, please connect to these addresses:

Issuer's app:
https://192.168.0.122:10443

RA's app:
https://192.168.0.122:9443

Verifier's app:
https://192.168.0.122:8443

rkvac-server login: _
```

Fig. 3.2: Server on startup

3.3.1 Personalization of the card

1. Connect to issuer's app on the address:
 - `https://<server-address>:10443`
2. Log in using credentials:
 - username – **admin**
 - password – **Vut2021**
3. Test the smart-card – on the home page you should see your smart-card reader listed on the panel „Smart-card readers“ (see Fig. 3.3). By clicking on the reader, application will test the inserted card with APDU_SELECT message.

Info: if you don't see your reader listed, please update Smart Card Extension or restart the browser.

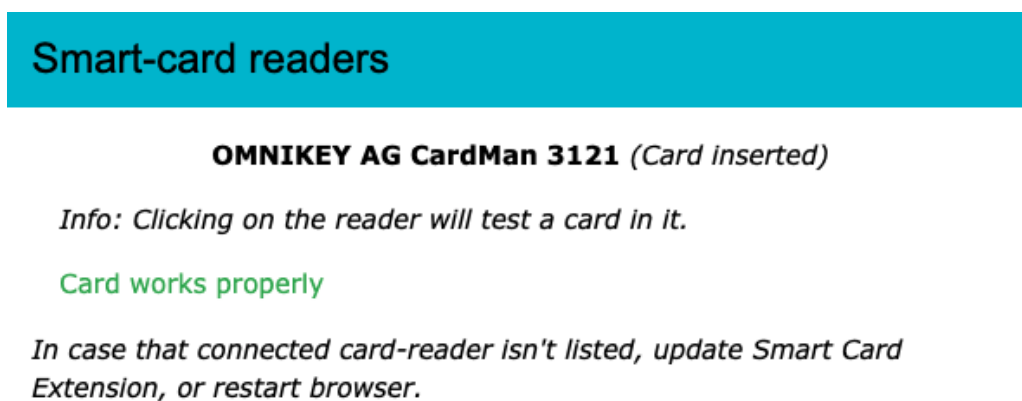


Fig. 3.3: Testing smart card

4. Navigate to page „Users“ using the menu bar on the top.
5. On the form „New User“ choose your smart-card reader and enter:
 - first name: **John**
 - last name: **Smith**
6. Click „Register“

7. If you see the success message and the new user is listed in the „User list“, the card personalization was successful (see Fig. 3.4).

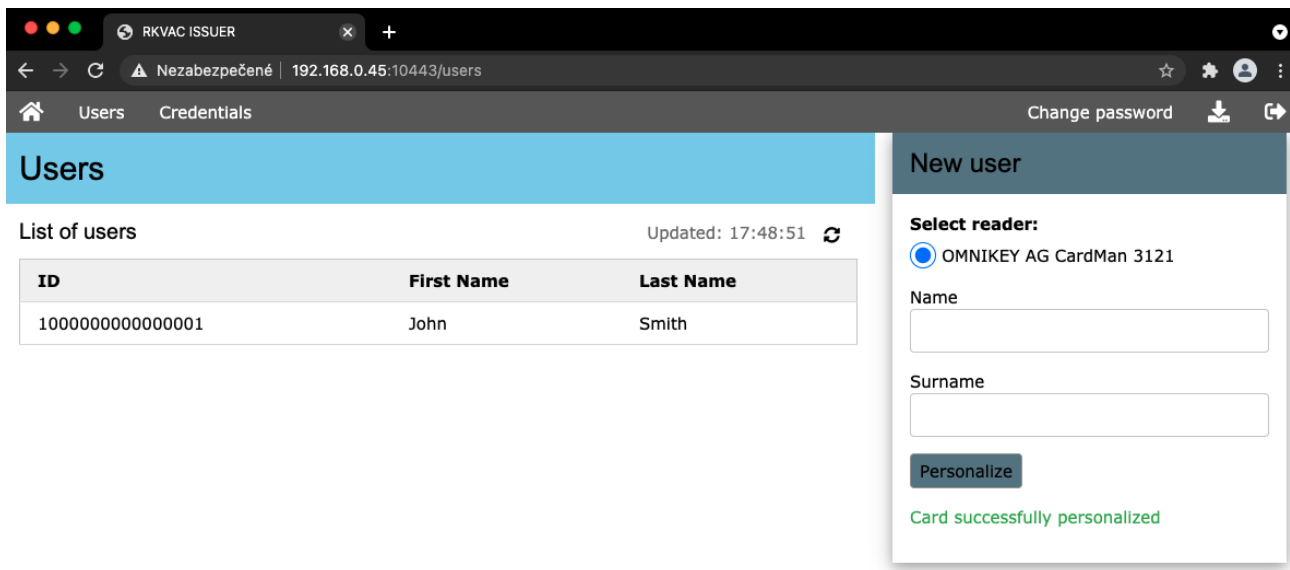


Fig. 3.4: Card's personalization

3.3.2 Assigning revocation handler

After personalization of the card, you need to assign a revocation handler to it.

1. Connect to revocation authority's app on address:
 - `https://<server-address>:9443`
2. Log in using credentials:
 - username – **admin**
 - password – **Vut2021**
3. Initiate the app using the initiate button.
4. Select your smart-card reader
5. Assign revocation handler to the card.
6. If you see the success message, the process was successful (see Fig. 3.5).

3.3.3 Permitting verifier

In order to allow connection from the verifier's app, you need to add his IP address to „Permitted verifiers“ list. Verifier will need to connect to RA's app during switching to new epoch (see 3.4.3).

1. Navigate to „Verifiers“ page using menu bar.
2. Add address **127.0.0.1** – verifier's application runs on a same machine, so it will use the localhost address.

List of permitted verifiers should look like Fig. 3.6.

Revocation handler

Select reader:

 OMNIKEY AG CardMan 3121 (Card inserted)

Card works properly

Info: Clicking on the reader will test the card in it.

In case that your reader isn't listed, please reload Smart Card Extension or restart browser.

Assign

Revocation handler successfully assigned to the card

Fig. 3.5: Assigning revocation handler

3.3.4 Managing the keys

During the first usage of the revocation authority's app, private and public keys were generated. In order to use the issuer's and verifier's app, you need to integrate some of these keys to their system.

1. Download `ra_pk.dat` and `ra_public_parameters` from panel „Revocation authority's files“.

Note: please be careful if you already have some other files in your `Downloads/` folder with the same name. You need to delete the old files, so that these actual files have the appropriate names.

3. Log into the issuer's app – you were probably log-out from this app, so you need to **refresh the page** and re-log in.
4. Import the `ra_pk.dat` to the issuer's system using „Tools“ panel.

After importing the appropriate file, you should see that the card „Credentials“ was turn to blue (see Fig. 3.7). This indicates that you have all dependencies set up and you can assign attributes to the card.

3.3.5 Assigning attributes

Using this example, the card will have assigned attributes, which will provide access to the verifier's system with role **teacher**.

1. Navigate to the „Credentials“ panel.
2. On the panel „New credentials“ choose „Own“.
3. Select your smart-card reader.
4. In the form enter these values:

Permitted Verifiers

Only hosts in this list are allowed to connect to revocation authority in order to activate their epoch

Verifier's IP Address

Add

Updated: 10:09:08


Host
127.0.0.1 

Fig. 3.6: Permitted verifiers

Tools

Description	File	Action
Issuer's private key	<div>Vybrať súbor</div> <div>Nie ...úbor</div>	<div>Upload</div>
RA's public key	ra_pk.dat	<div>Delete</div>

Fig. 3.7: Importing RA's keys

- Name – **JohnSmith**
 - Attribute count – **4**
 - Attribute 1 – **John Smith**
 - Attribute 2 – **Male**
 - Attribute 3 – **vut-teacher**
 - Attribute 4 – **db-teacher**
5. Click „Assign“.
 6. If you see the success message and you can see the file **JohnSmith.att** in the credentials list, the process was successful (see Fig. 3.8).

3.4 Verifying attributes

In this section the verifier's app will be set up to grant the teacher's access for user's that can proof, that hold attributes **vut-teacher** and **db-teacher** on the positions **3** and **4** of theirs credentials.

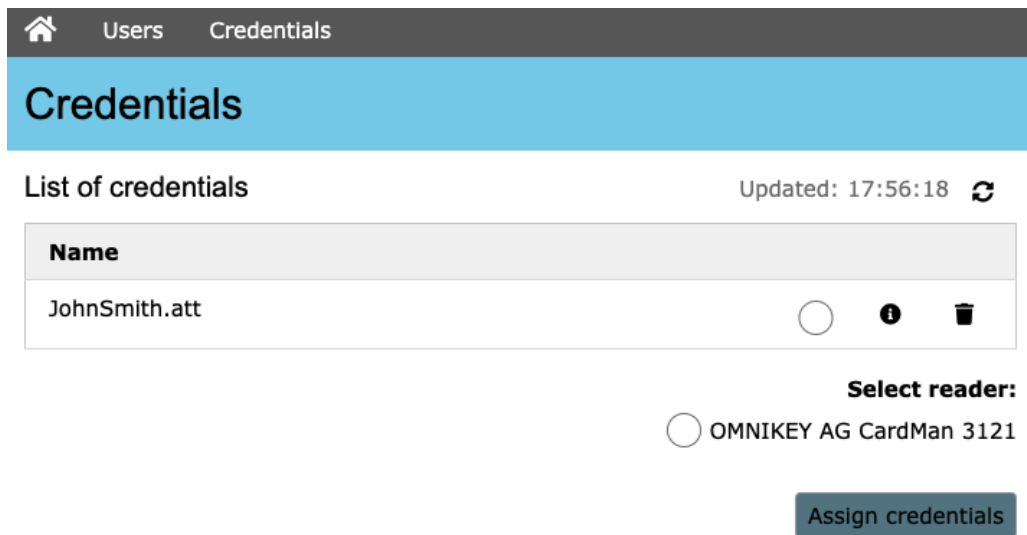


Fig. 3.8: Created new credentials file

3.4.1 Integrating verifier to RKVAC

As a first step, you need to integrate the verifier to the RKVAC system. This can be done by importing revocation authority's public files and issuer's private key into the verifier's system.

1. In issuer's app, navigate to the home page.
2. Download `ie_sk.dat`.

You should have the revocation authority's public files downloaded from earlier. If not, please see subsection 3.3.4.

4. Connect to verifier's app at the address:
 - `https://<server-address>:8443`
5. Log in using local authentication and credentials:
 - username – **admin**
 - password – **Vut2021**
6. Navigate to „Settings“ using the left panel.
7. Initiate the app using the appropriate button.
8. Import the downloaded files to the system using „RKVAC keys“ panel.

3.4.2 Preparing access credentials

Using these steps you will prepare access credentials for teacher's access. Similarly you can later prepare credentials for both admins and students.

1. On the panel „New credentials“ choose „Teacher“.
2. In the form enter these values:
 - Attributes count – **4**
 - Attribute 1 – leave empty
 - Attribute 2 – leave empty

- Attribute 3 – **vut-teacher**
- Attribute 4 – **db-teacher**
- Required attributes position – **3,4**

3. Click „Create“

In the result the prepared teacher’s credentials should look like Fig. 3.9. You can check credentials details through the table above, where this credentials should be marked as **ready**.

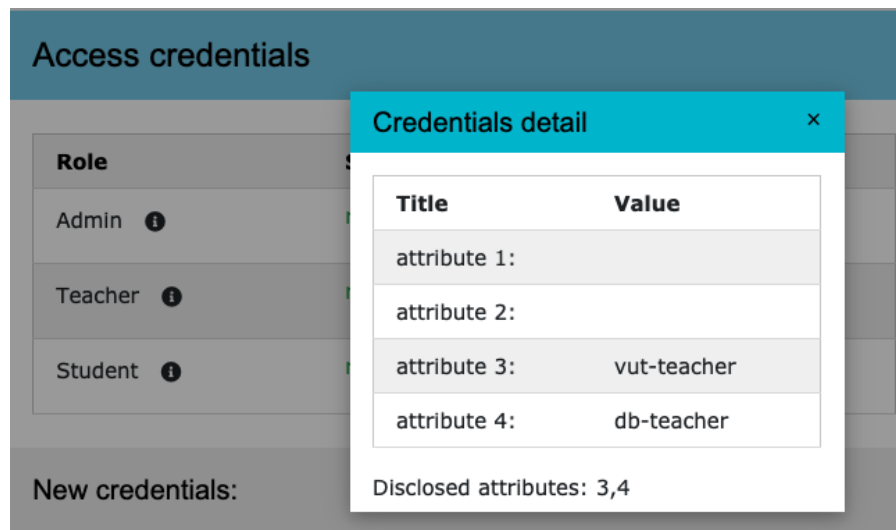


Fig. 3.9: Teacher’s access credentials

3.4.3 Connecting to RA

In this subsection you will finalize verifier’s settings by connecting it to revocation authority’s server.

1. In the panel „Epoch settings“ in the revocation authority’s address field enter **127.0.0.1**
2. Click „Save“
3. Click „Change now“

After following these steps, the revocation authority’s address (in this case localhost) is saved to the verifier’s system and a new epoch was successfully generated (see Fig. 3.10).

At this point you have everything set up for successful authentication. Log out from the verifier’s app and on the login page choose your smart-card reader and click on „Teacher“ button. This will start the verification process. If everything was correctly set up, you should be logged in the app with teacher’s access.

Epoch settings

Current epoch:

01070521

Switch now

Revocation authority's address:

127.0.0.1

Save

Delete

Revocation authority's address saved

Fig. 3.10: Epoch settings

3.5 Revoking user

In this section you will revoke the card from the RKVAC system. There are two possibilities on how to revoke user:

- using **user's ID**
- using **user's pseudonym C** and **epoch number**

Using these steps, you will revoke user using his **pseudonym C** and current epoch number.

1. Log into the verifier's application as Admin (using local authentication).
2. Navigate to „Access logs“ page using left menu bar.
3. Write down **Epoch number** and **Pseudonym** from the last log (see Fig. 3.11).



Access logs					Logged in: <i>admin</i> 
 Last update: 10:01:47					
Day	Time	Epoch number	Pseudonym	Result	
Fri May 7 2021	10:01:33	01070521	db6ddd075d4fa5540b5a9d7648f48ca2939f53d560249208510e9a963c27a493	ALLOWED	

Fig. 3.11: Access log

4. Log into the revocation authority's app.
5. On panel „Revocation of user“ enter:
 - **User's ID** – leave empty.
 - **Pseudonym C** – user's pseudonym from access log.
 - **Epoch number** – epoch number from access log.

- **Verifier's address** – leave empty – if left empty, localhost address is automatically used.
6. Click „Revoke“.
 7. If the revocation was successful you should see an appropriate message (see Fig. 3.12).

Revocation of a user

User's Identifier:
1000000000000001

User's pseudonym C:
db6ddd075d4fa5540b5a9d7648f48ca2939f53d560249208510e9a963c27a493

Only one of pair identifier-pseudonym can be specified.

Epoch number:
01070521

Verifier's address:
127.0.0.1

In case of multiple verifiers separate addresses with commas

User successfully revoked from system

Fig. 3.12: Revocation of a user

At this point your card should be revoked from the system. Connect to verifier's app and try to log in as „Teacher“, using your smart card. At the end of the verification process, you should see message „Access denied“. In case you want to add this card to the system, you need to follow all steps from section 3.3.