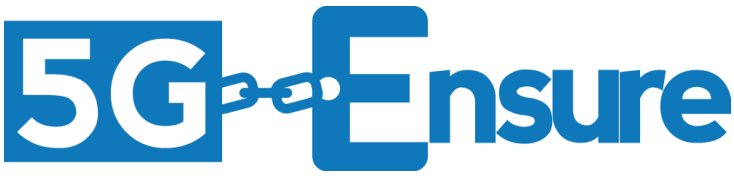

Deliverable D3.8
5G-PPP Security Enablers Documentation (v2.0)
Enabler Privacy Policy Analysis

Project name	5G Enablers for Network and System Security and Resilience	
Short name	5G-ENSURE	
Grant agreement	671562	
Call	H2020-ICT-2014-2	
Delivery date	31.08.2017	
Dissemination Level:	Public	
Lead beneficiary	NEC	Felix Klaedtke, felix.klaedtke@neclab.eu
Authors	IT Innovation: Gianluca Correndo, Yoana Paleva, Toby Wilkinson	

Document Version	Date	Change(s)	Author(s)
0.1	02.06.2017	Created template	Felix Klaedtke
0.2	04.08.2017	Initial draft	Yoana Paleva, Toby Wilkinson
0.3	23.08.2017	Updated user guide	Yoana Paleva
1.0	24.08.2017	Final version	Gianluca Correndo, Toby Wilkinson

Foreword

5G-ENSURE belongs to the first group of EU-funded projects which collaboratively develop 5G under the umbrella of the 5G Infrastructure Public Private Partnership (5G-PPP) in the Horizon 2020 Programme. The overall goal of 5G-ENSURE is to deliver strategic impact across technology and business enablement, standardization and vision for a secure, resilient and viable 5G network. The project covers research and innovation - from technical solutions (5G security architecture and testbed with 5G security enablers) to market validation and stakeholders' engagement - spanning various application domains.

This manual is part of the project's deliverable D3.8. It describes how the Privacy Policy Analysis Enabler is installed and administrated within the work package 3 of the 5G-ENSURE project. Furthermore, this manual contains a user guide of the privacy enabler.

Disclaimer

Copyright notice

Contents

1 Introduction

Nowadays, users of networked services are confronted with a wide range of services and applications which may put their privacy at risk.

With this ever-increasing availability of services based on the 5G infrastructure, the potential exposition of personal data to unintended actors is a growing concern. Typically, users don't spend too much time reading services' privacy policies and have therefore little understanding of how their personal data may be accessed and used by a service, and for what purpose. The verbose textual privacy policy statements provided by services providers ensure legal compliance, but are of little help to users which usually disregard them.

This enabler aims to provide the user a way to analyse the privacy policies of a set of services or service providers in order to inform the users on how their privacy is handled. The analysis would usually be carried out prior to the service being used.

This enabler allows the user to specify their privacy preferences including what type of data they are willing to share, for what purpose and for what period. This allows the user to make privacy aware decisions regarding use of 5G services. The enabler may be of interest to all 5G users.

2 Installation and Administration Guide

The enabler is provided as dockerised application which fully specify the dependencies needed by the enabler. This means that in order to install and run the enabler it is required to have a Docker environment which is enabled to open connections from the host to the network.

The installation package contains, once unzipped, the following folder structure:

```
.
├──client
└──server
    └──data
        ├──auth
        ├──policies
        └──semantic
```

This folder structure will be used as reference in the following subsections to describe the installation procedure.

2.1 System Requirements

The enabler requires a Docker system version 17.06.0 installed and working. The hosting server can be any supporting the stated Docker version although Ubuntu 16.04 is advised.

2.2 Enabler Configuration

The Privacy Policy Analysis enabler is a web application which allows to import privacy policies, specify user preferences, and search for policies as defined in the use cases sections of deliverable D3.6, section 3.4.8 [1].

The initial configuration provided by a fresh installation provides the default accounts provided to the users to test the enabler. The default accounts have different roles to allow the testing of different system's capabilities and are the followings:

Table 1 - Default users

username	email	password	role	description
admin	admin@privacy.org	privacyadmin	Administrator	Root user who can manage users and polices.
manager	manager@privacy.org	privacymanager	Privacy manager	User who can manage privacy policies
user	user@privacy.org	privacyuser	User	User who can specify privacy preferences and search for policies.

2.3 Enabler Installation

The installation process restores the client and server docker images onto the host's Docker system and start the containers to serve the enabler from the localhost. The installation procedure is as follows:

1. Unzip the privacy enabler deployment tar.gz file:

```
tar -zxvf privacy-analysis-enabler.tar.gz
```

2. Cd into the server folder:

```
cd privacy-analysis-enabler/server
```

3. Build the server side:

```
./build.sh
```

4. Once this step has been done there should be a new image available to Docker tagged "privacy-enabler:rest". Check by running the following command and check that the information formatted in bold are present:

```
docker images

REPOSITORY          TAG      IMAGE ID       CREATED      SIZE
privacy-enabler     rest     d97b7b9509bc   5 days ago   222MB
```

5. Cd into the client folder:

```
cd ../server
```

6. Build the client side:

```
./build.sh
```

7. Once this step has been done there should be a new image available to Docker tagged “privacy-enabler:ui”. Check by running the following command and check that the information formatted in bold are present:

```
docker images

REPOSITORY          TAG      IMAGE ID       CREATED      SIZE
privacy-enabler     rest     d97b7b9509bc   5 days ago   222MB
privacy-ui          ui       aeff0ec1289e   5 days ago   16.7MB
```

8. Now that the two Docker images are available in the system it is possible to instantiate them and access the application:

```
> cd ..
> ./run.sh
```

9. The application should be available under http://localhost/. The application has been developed using Firefox 54.0.1 (32-bit) and Chrome 60.0.3112.101 (64 bit).
10. In order to stop the enabler, go to the terminal in which the enabler has been started from and issue a “CTRL+C” command.

2.4 Troubleshooting

At each step in the previous section the error messages are relevant to the Docker documentation.

3 User and Programmer Guide

3.1 User Guide

In this section we describe the functionality of the Privacy Enabler which implements the use cases described in deliverable D3.6 [1].

3.1.1 Main page

On the main page of Privacy enabler (Figure 1) there is a navigation bar at the top of the page containing two links: FAQ and Contact us. The FAQ link takes the user to a page with frequently asked questions with answers if the user needs more information, and the Contact us link takes the user to a page with contact information. In the center of the page there are to more links: Log in and Sign up. The Log in link takes the user to the log in page if the user already has a profile. The Sign up link will take users that are new to the service to the sign up page. At the bottom of the page there is information about Privacy Enabler: what it offers to the user and why these services are beneficial to them.

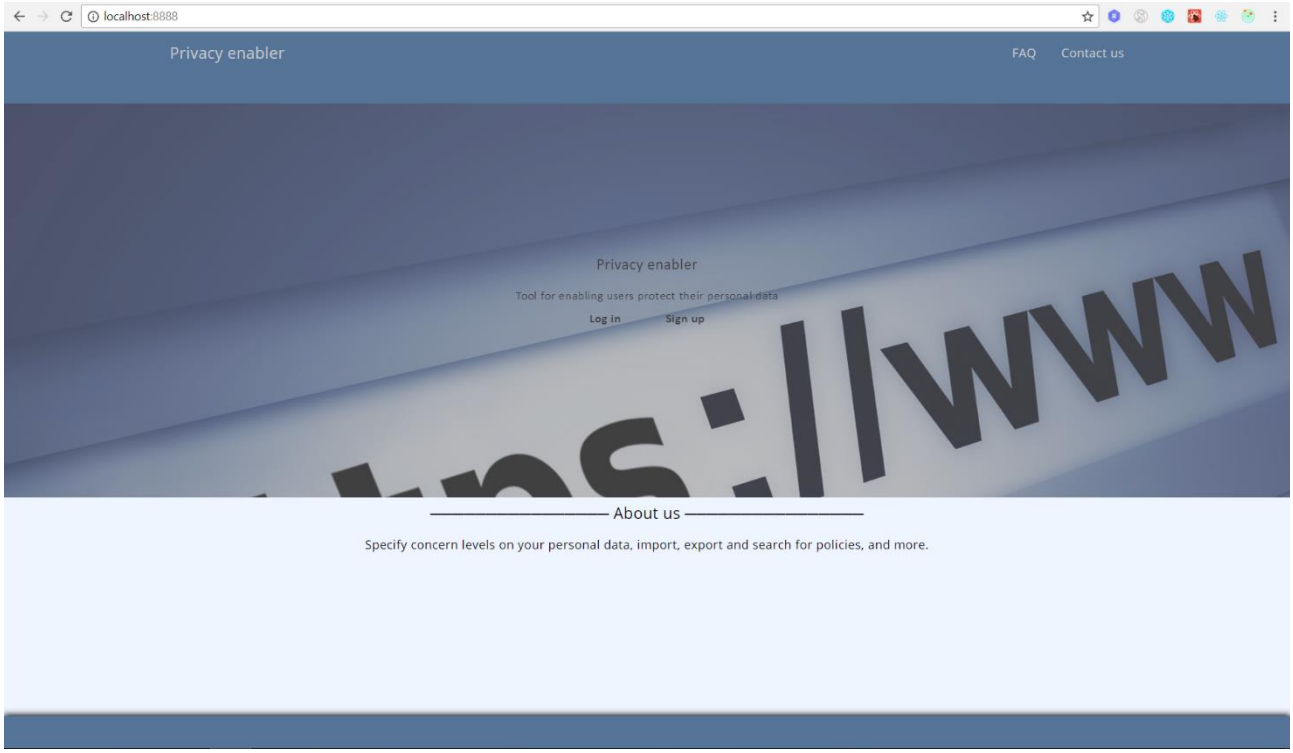

Figure 1 - Privacy enabler main page

3.1.2 Login page

In order for a user to log in they should already be registered and should provide the email address and password used when creating the account. On log in the user will be redirected to the Home page of Privacy Enabler.

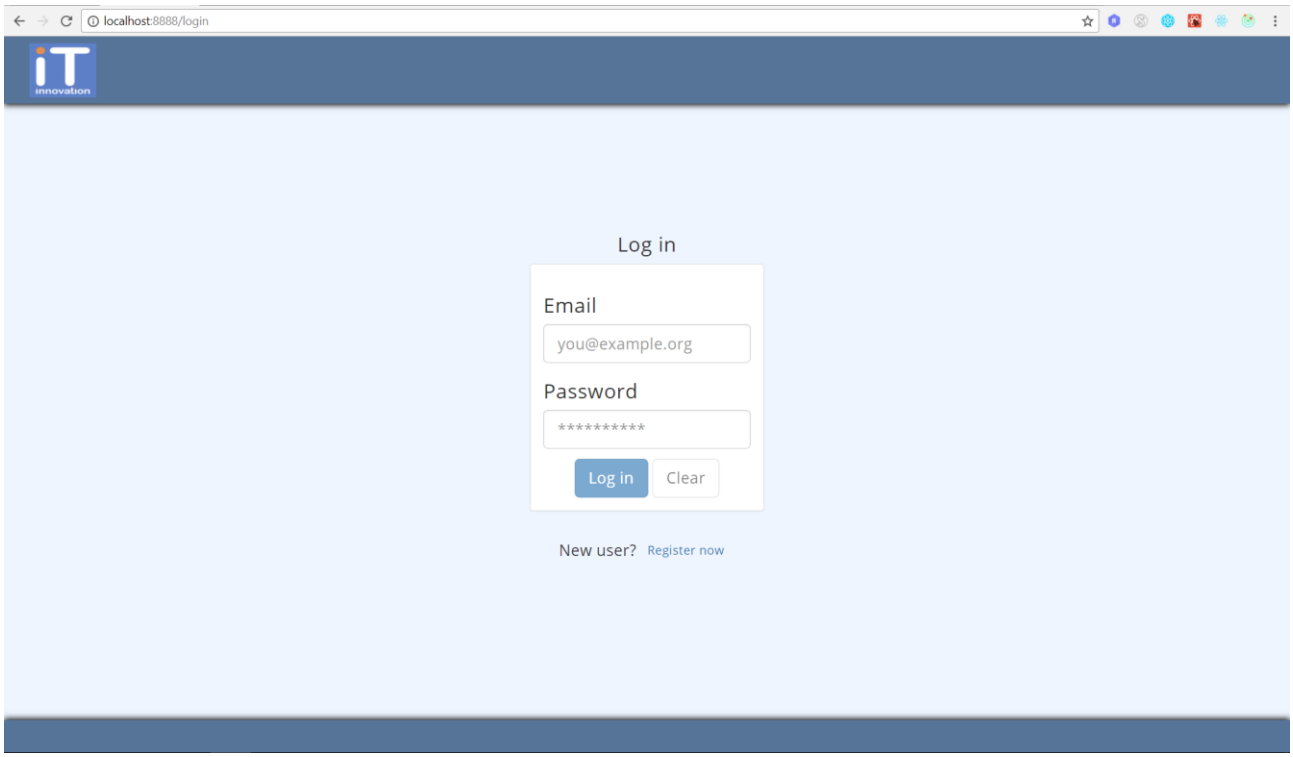

Figure 2 – User login page

3.1.3 Signup page

The user can register by providing a unique username, valid email address and secure password filling in the confirm password field for security reasons. The user should also provide their first and last name. After clicking on Sign up the user is redirected to the Login page where their email address and password will be required.

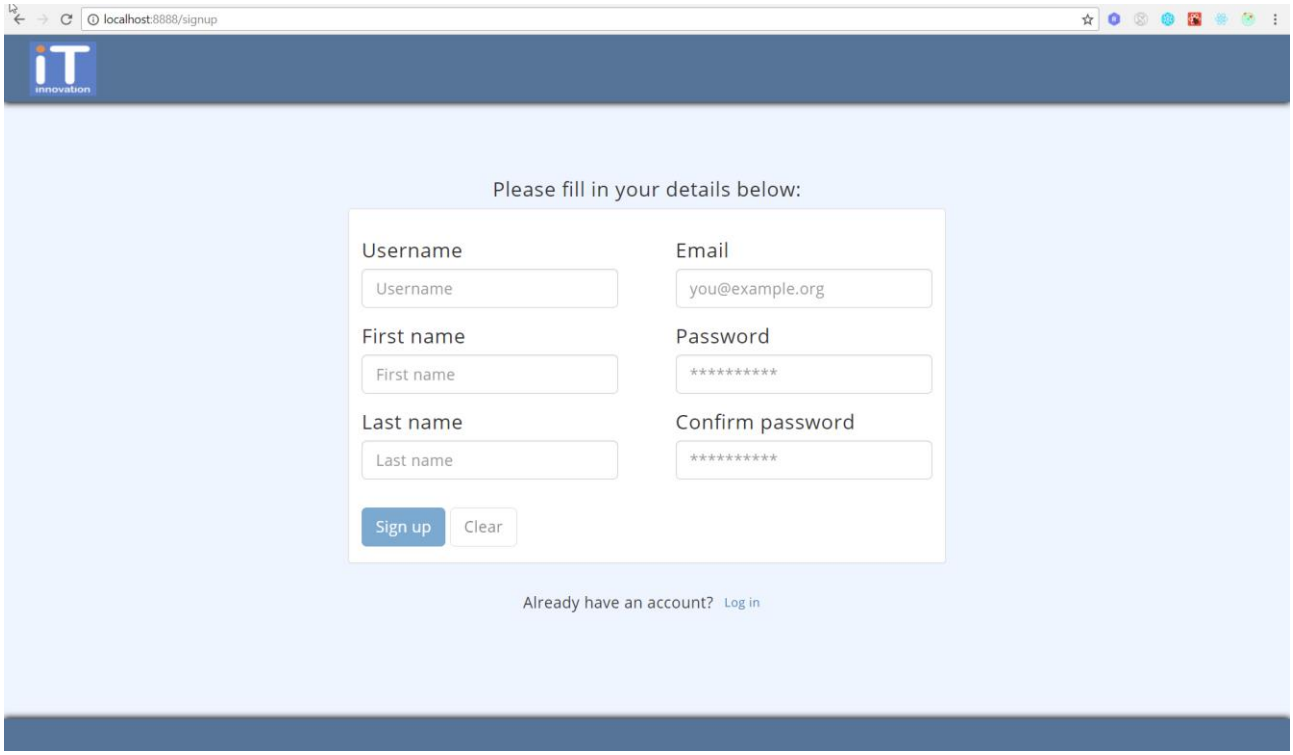

Figure 3 - User registration

3.1.4 Home page

After the user has logged in he is redirected to the home page, which contains information about the app, what kind of services it offers and links to them.

- The Questionnaire panel contains brief information about the Privacy Enabler service which allows the user to specify concern levels on their private data which is going to be accessed by certain roles, depending on the domain of the service which the user wants to use/ subscribe to. The link will take the user to the Preferences page, containing more information on how the data is collected, how the questionnaire is constructed and why it is the main and most important service of Privacy Enabler.

- The Search panel gives the user a brief description of how the search service works and why it is helpful. This service will let the user find compliant policies depending on their preference: 1 meaning unconcerned about the score of the policy and 10 meaning very concerned, accordingly. The policy score is calculated taken the types of data the service provider wants to access and the purpose of the data access. The link will take the user to the Search page where the user can do the privacy policy search.

- The Import panel describes how the importing of new policies is implemented and how the user can select a new policy and upload it to the server. After that there is a brief description of how the user can visualize the policies they own and see the details of each, export or delete it. The link is to the Import page where the user can upload the policies they want.

- The My account panel describes what kind of information the user will find in Privacy Enabler and how the user can manage their account. The link is to the user profile page.

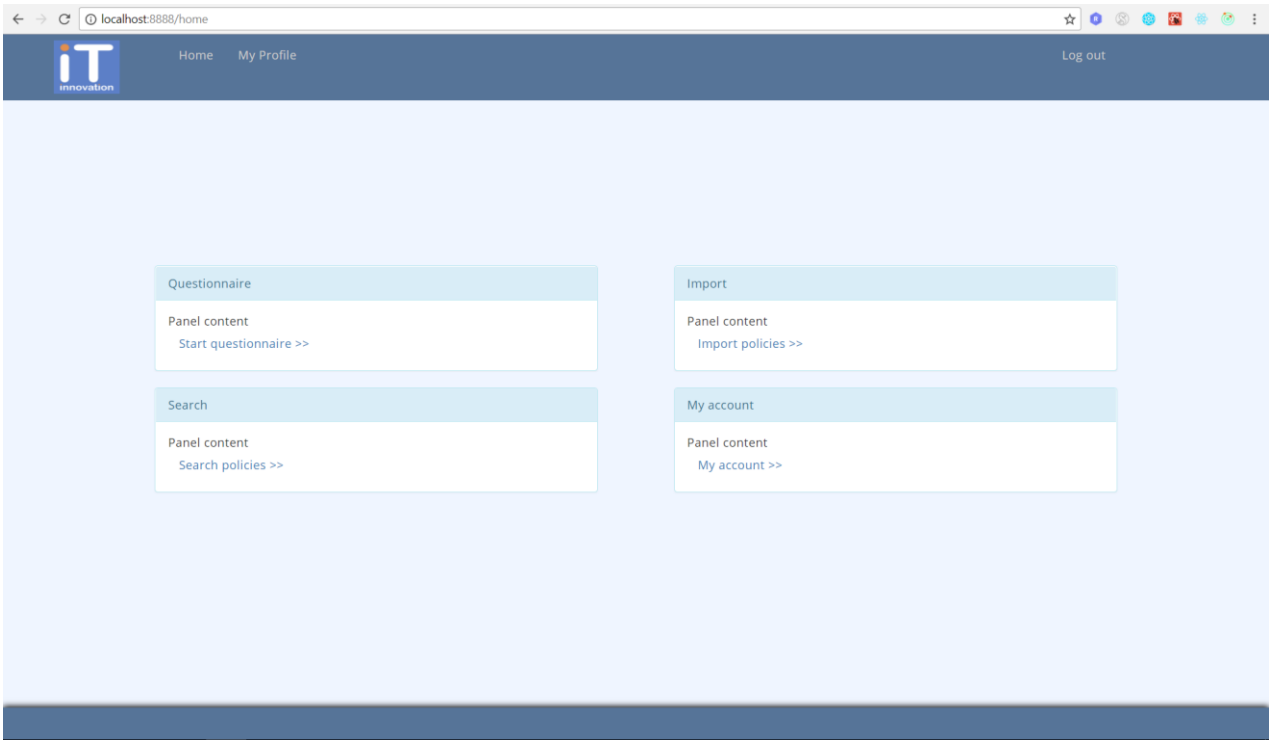

Figure 4 - Home page

The account page contains a summary of user's information and the user menu:

Figure 5 – User profile page

The navigation at the top of the page contains three links: Home, My Profile and Log out. The Home and My Profile links will take the user to the Home page and the user's account page accordingly at any point. By clicking on Log out the user can log out of the app at any point and will be redirected to the login page.

The navigation bar on the left of the page is the menu containing links to all of the services Privacy Enabler offers.

- Search

This link will take the user to the Search page.

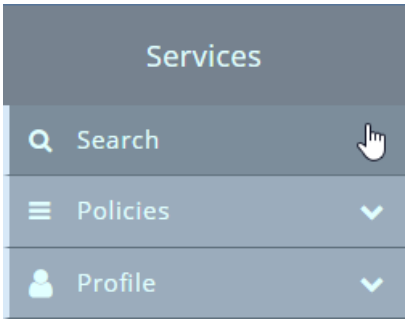

Figure 6 – Policy search link

- Policies

A dropdown link containing two links:

- Import new policy

This link will take the user to the Import page.

- My policies

This link will take the user to the Policies page, where all of the user's owned policies will be listed.

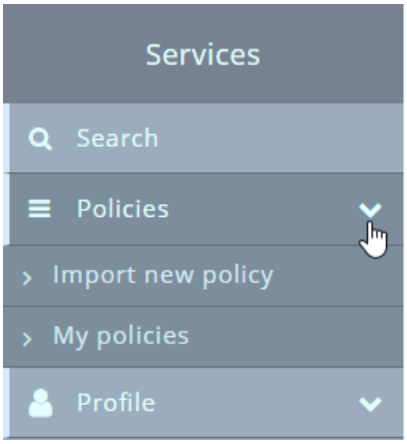

Figure 7 – Policies dropdown link

- Profile

A dropdown link containing one link:

- Specify preferences

This link will take the user to the Preferences page, which contains a link to the Questionnaire page. The latter is where the user will be able to specify concern levels on their private data.

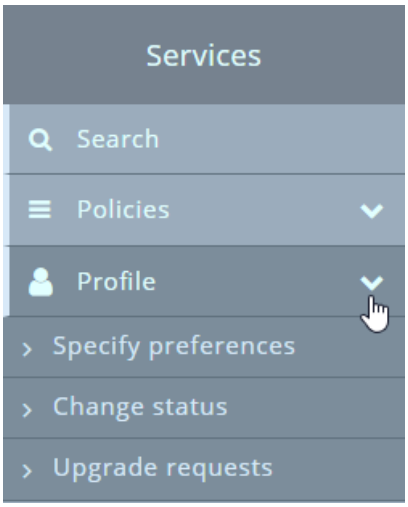

Figure 8 – Profile dropdown link

3.1.5 Search page

This page doesn't require a special status and all users can access it from the navigation bar on the left. This service will let the user find compliant policies depending on their preference: 1 meaning unconcerned about the score of the policy and 10 meaning very concerned, accordingly. The policy score is calculated taken the types of data the service provider wants to access and the purpose of the data access. It is visualized by a slider bar which the user can move in order to specify their level of concern. 1 puts the user in the category "Unconcerned" and 10 puts them in the category "Fundamentalist". The more concerned the user is about their data, the more policies are going to become non-compliant and go in the Noncompliant table.

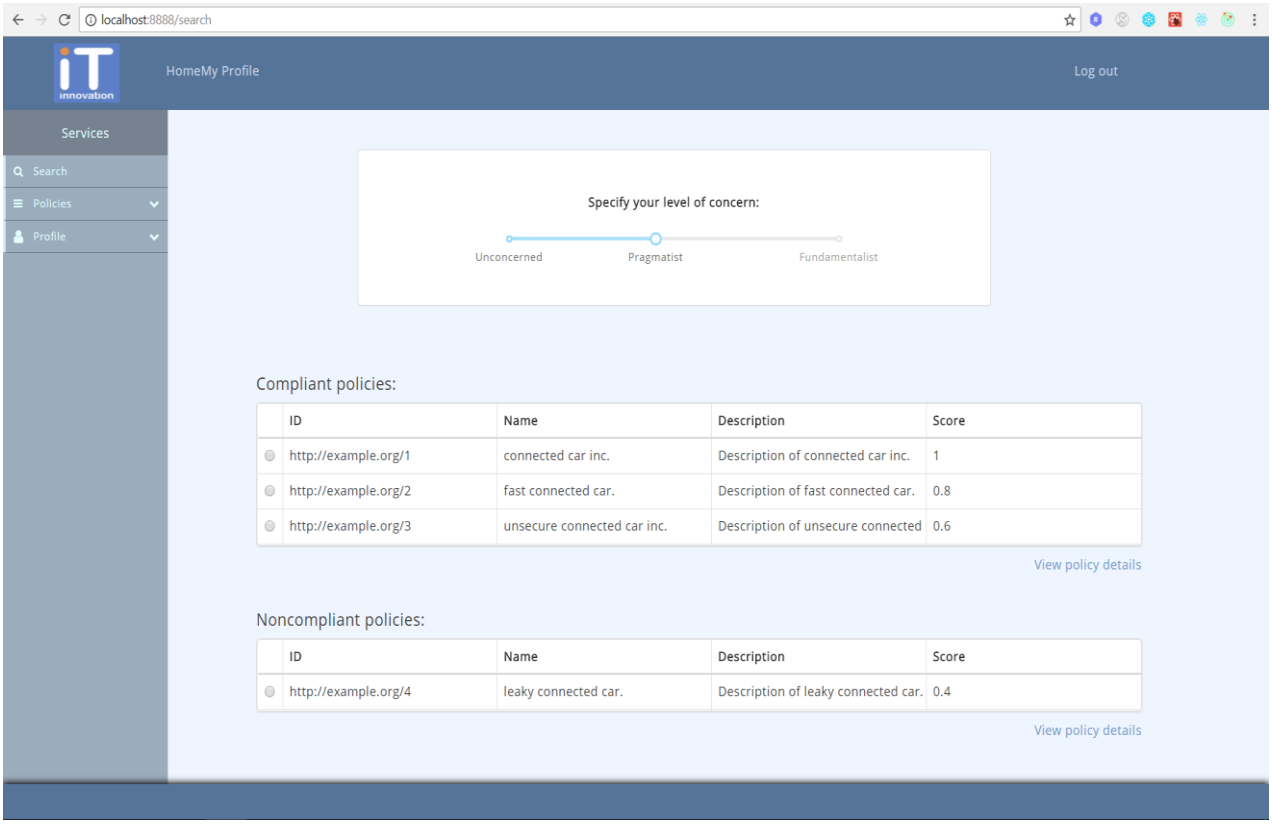

Figure 9 – Search page

As you can see on Figure 10 below, as the user moves the slider bar policies move from one table to the other. In this example the user is lowering their level of concern of their personal data, meaning more privacy policies will become compliant. This means that the lower the user level of concern is, the more services will become eligible for a potential provider for that user. The View policy details link below both tables will take the user to the Policy details page, which lists all the details about the certain policy the user has selected from the table.

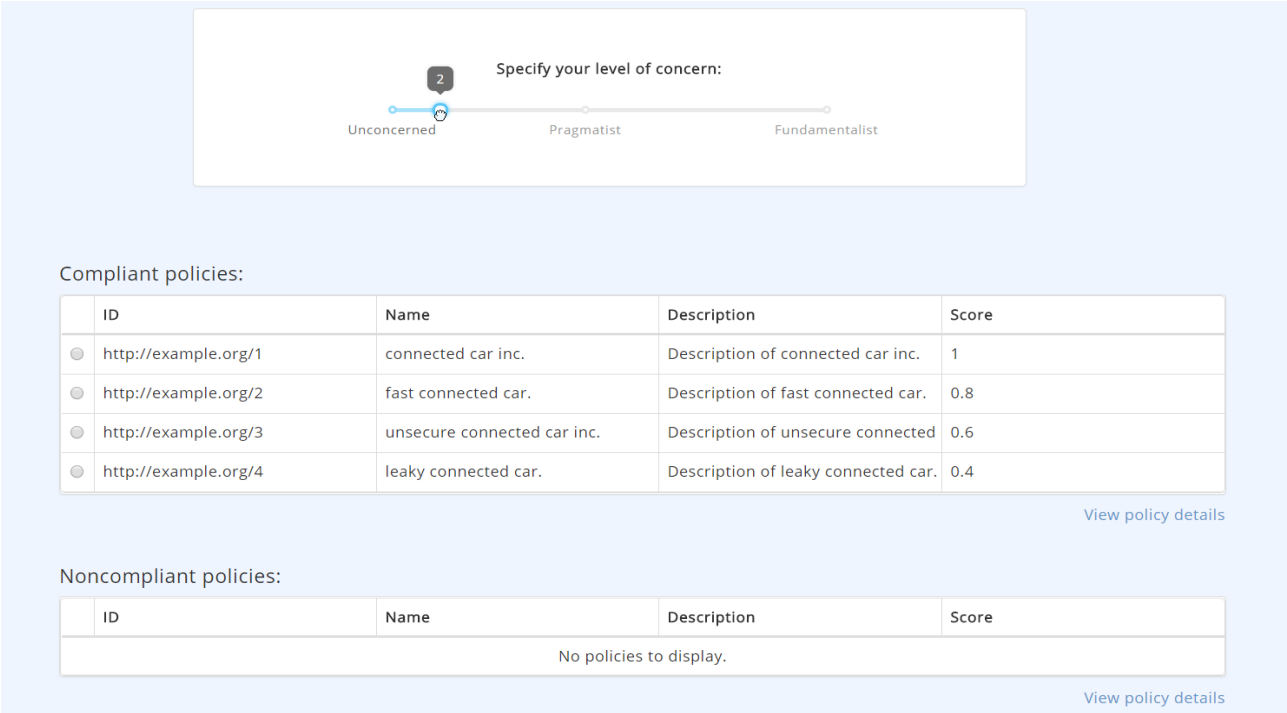

Figure 10 – Moving the slider bar

3.1.6 Import page

This page requires a special status and only user that have acquired the Privacy Manager role or are the system administrator can access it from the navigation bar on the left. The Import page allows the user to import new policies by uploading a file from their local storage. By importing a policy the user will add it to their own privacy policy list, which they will be able to see on the Policies page.

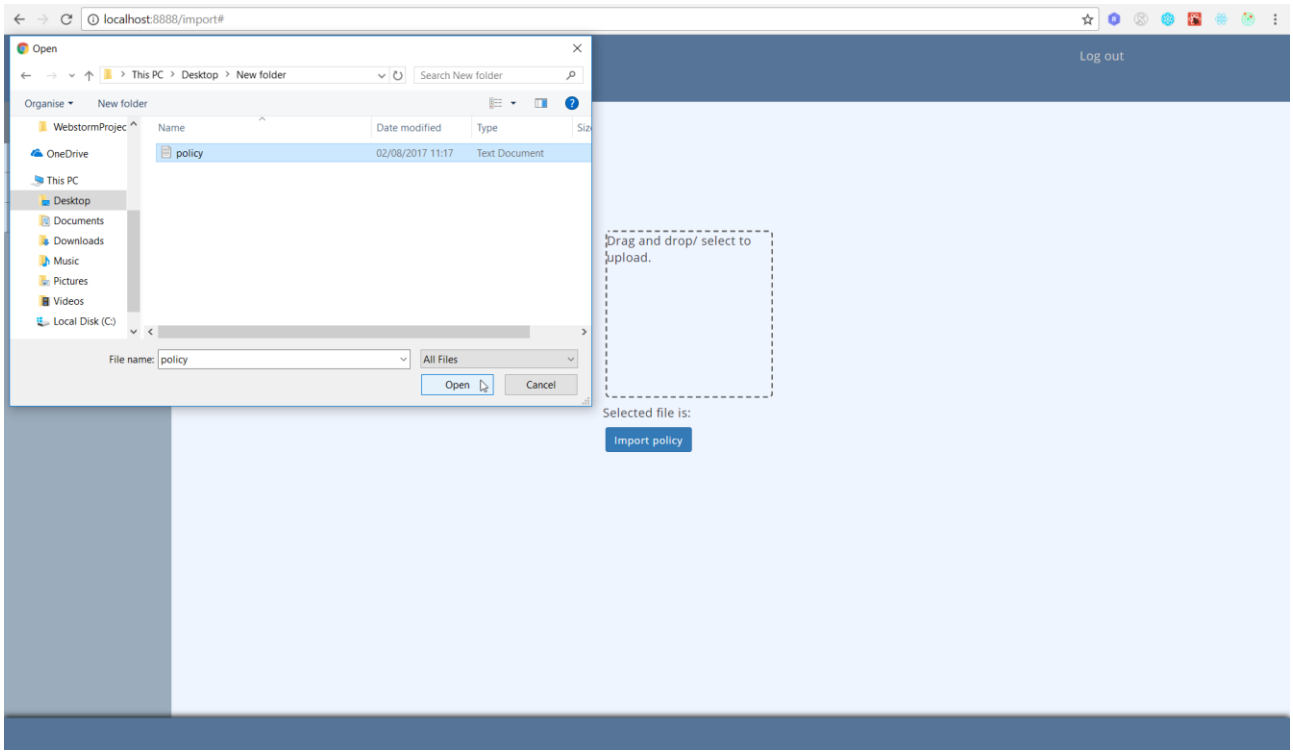

Figure 11 – Choosing a policy

Figure 12 – Importing the new policy

3.1.7 Policies page

This page requires a special status and only user that have acquired the Privacy Manager role or are the system administrator can access it from the navigation bar on the left. The Policies page allows the user to see the policies they own. By clicking on a policy the user can delete, export and view the details of the selected one. The user can also search a policy by its ID. Deleting the policy will result in the policy being removed by the user's owned privacy policies and therefore it will stop being available. Exporting a policy will result in the form of a valid RDF file with the policy's details. Viewing a policy's details will redirect the user to the View Policy page, where information about the policy will be displayed in more detail.

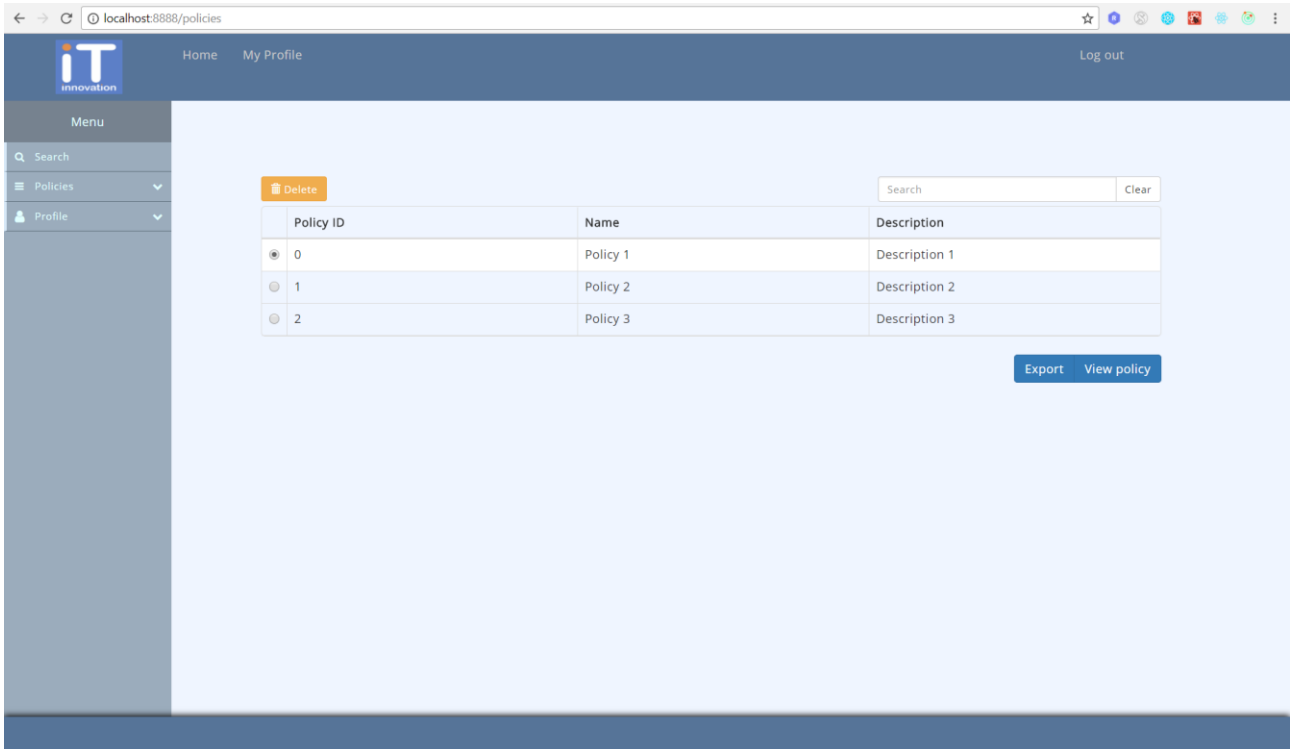

Figure 13 – List of user's policies

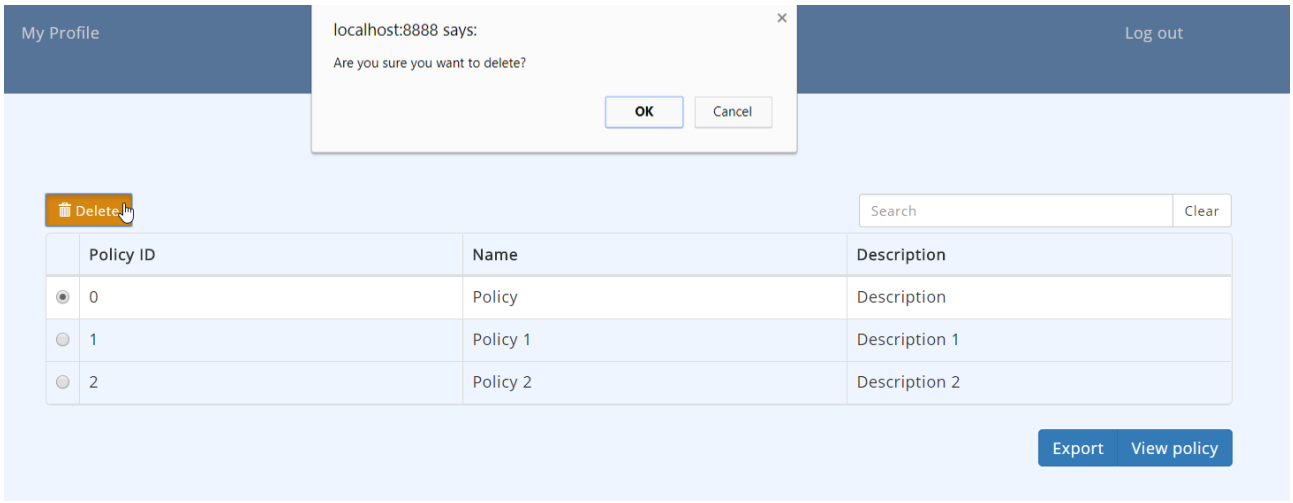

Figure 14 – Deleting a policy

Figure 15 – Find policy by Policy ID

3.1.8 View Policy page

This page's purpose is to act as a visualization for a selected policy. This doesn't require a special status and all users can access it from the Search page by selecting a policy and clicking on the View policy details link below the two tables on the page or if the user has acquired the Privacy Manager or Admin status they can also access that page from the Policies Page which lists their privacy policies uploaded to the system.

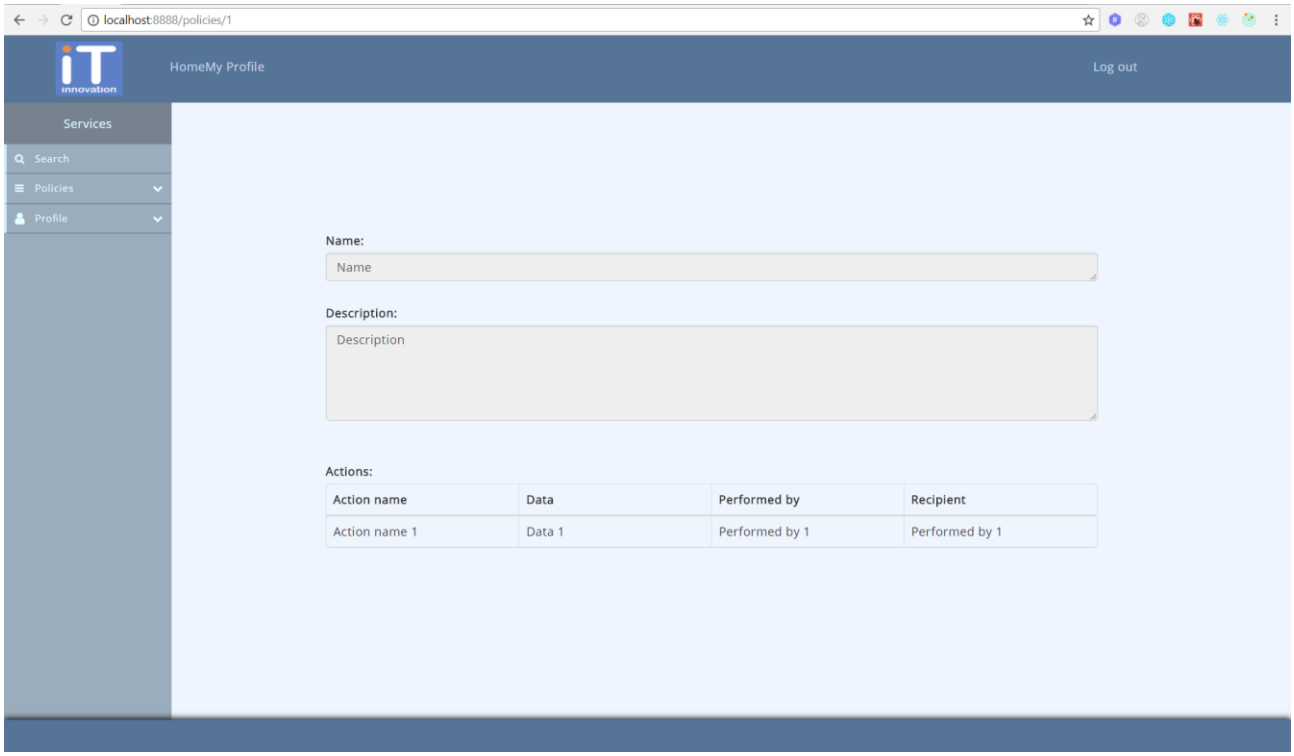

Figure 16 – View policy details page

3.1.9 Preferences page

This page is like an introduction to the main page of Privacy Enabler (Questionnaire page). It describes in detail how the questionnaire is constructed, what is its purpose, how does it affect the search for policies. It also contains a link activating the questionnaire.

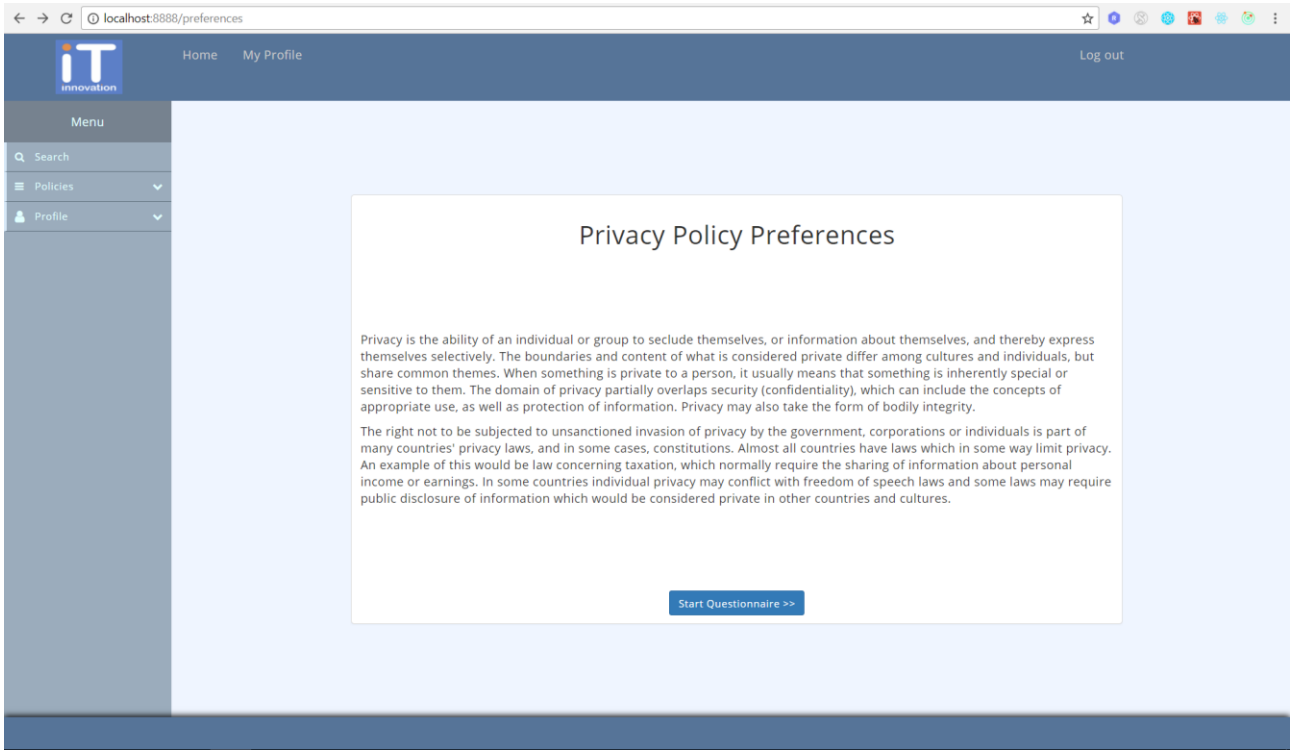

Figure 17 – Preferences page

3.1.10 Questionnaire page

The Questionnaire page is displaying a set of questions on which the user has to answer by moving the slider bar to the left or right depending on how concerned they are about their personal data. The default value for each question is 5, in case a user wants to skip a question. The further to the right the user moves the slider bar the higher level of concern is set to the certain question and the other way around. The higher the level of concern is, the less access to the user's private data will be allowed to the services. The questions are constructed by combining the types of data the service wants to access, the actions those services want to apply to the data they are accessing and the role they need to share the data with. It involves all the possible combinations data types, action types and roles that could possibly be required from the service. This way the user knows exactly what kind of information might be required from them in order for them to subscribe to/ use a certain service. After the questionnaire is done, the user will see a table listing all the questions with the user's level of concern on each. If the user doesn't have anything to change, he can submit their answers, if not they can start the questionnaire again.

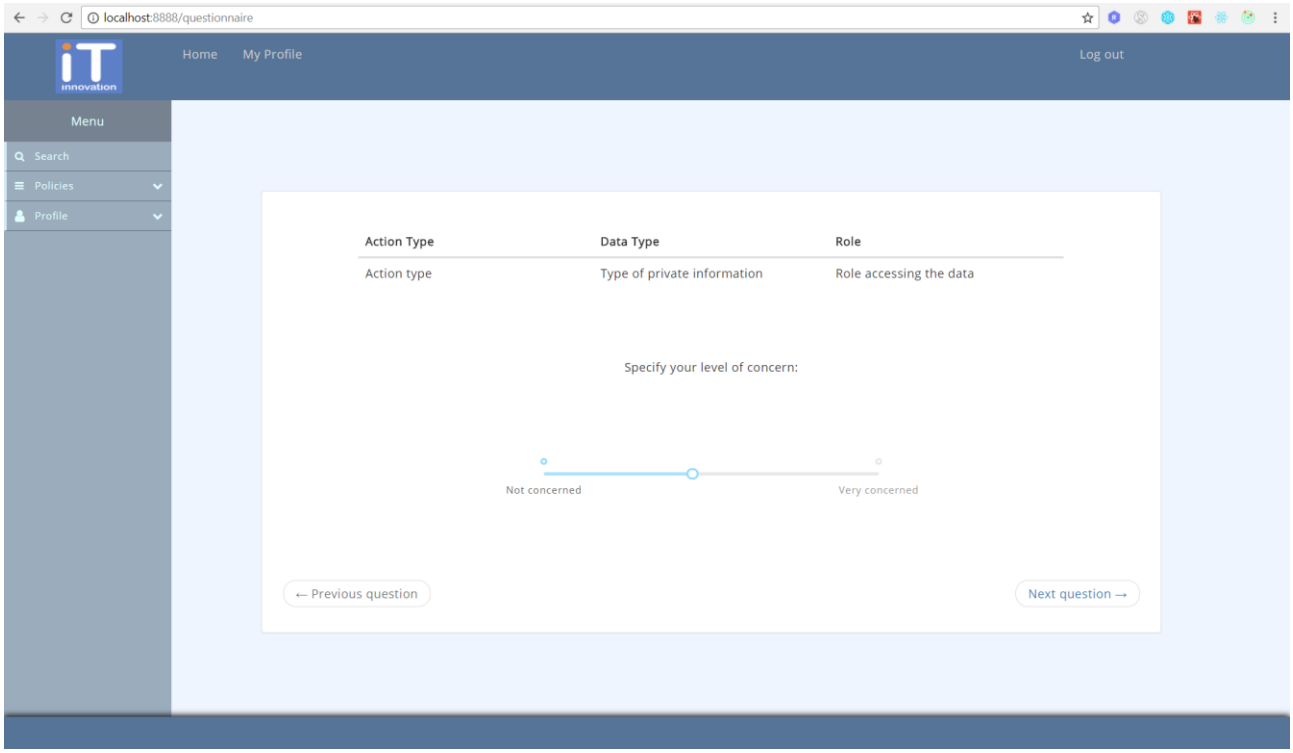

Figure 18 – Questionnaire page

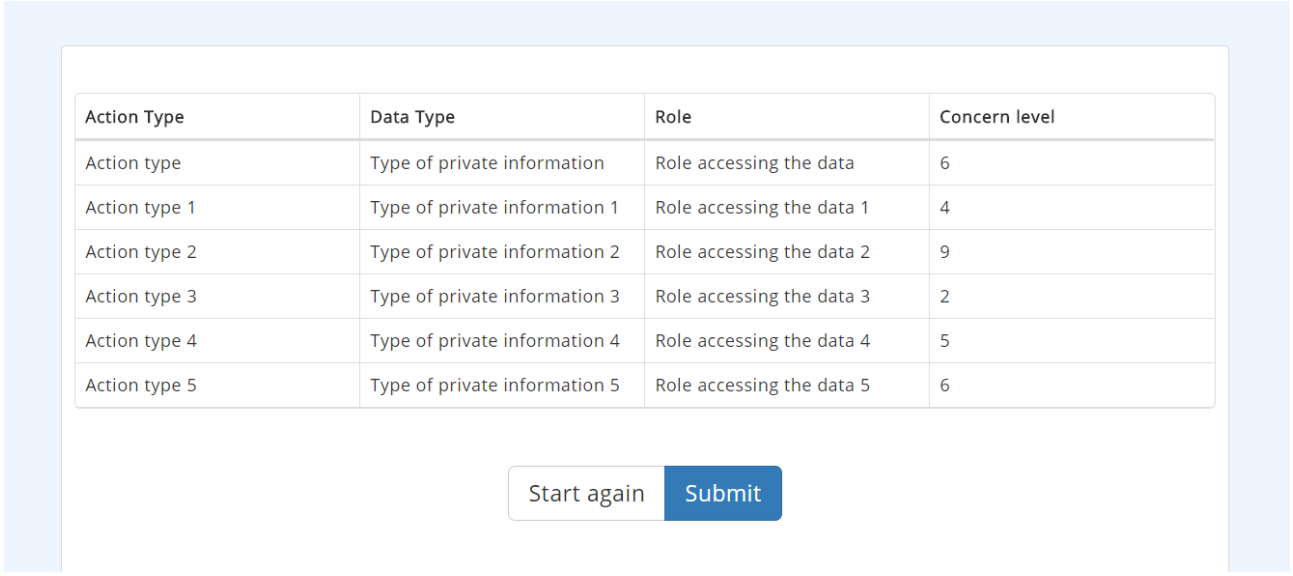

Figure 19 – Submit table with user preferences

3.1.11 Change Status Page

The Change status page can be accessed by the navigation bar on the left (Profile -> Change status). It contains brief description about how the user can change their status and what other services will be available after the request is accepted. The panel describes what options does the user have and what is the benefit of each, as well as special requirements and exceptions. For example a user's request to update their status to Privacy Manager might be declined. In this case the user can make another request shortly after. Another example is that a user might not be eligible to request a status upgrade to a System Administrator. In this case the user might have to upload more policies or check if there is an update on the requirements

in the description panel. The page also shows the current status of the user. If a user wants to make the status change request they should press the Continue button. If not, the Go back button which will take them to their account page.

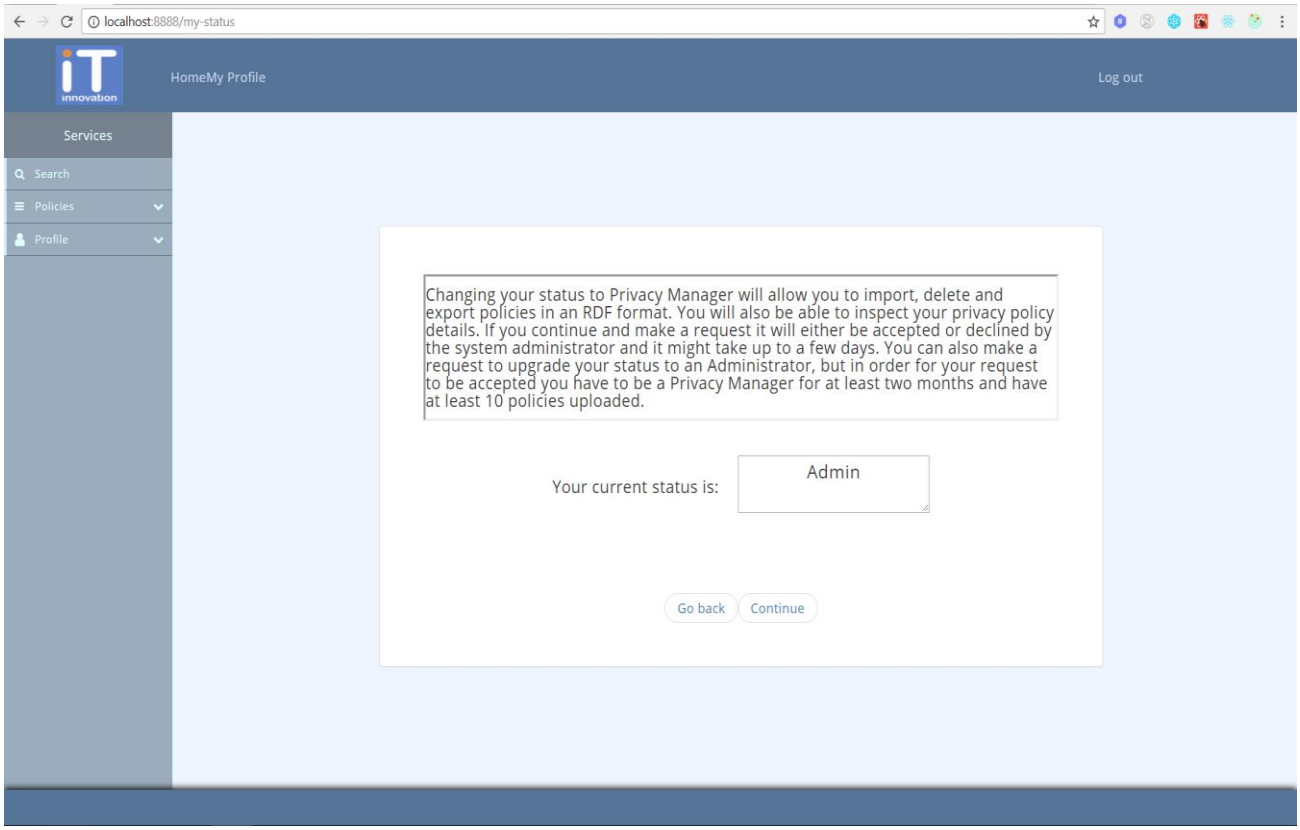

Figure 20 – Change status page

The continue button will display a new panel with a dropdown button containing the options of the user as depicted on Figure 21 (see below):

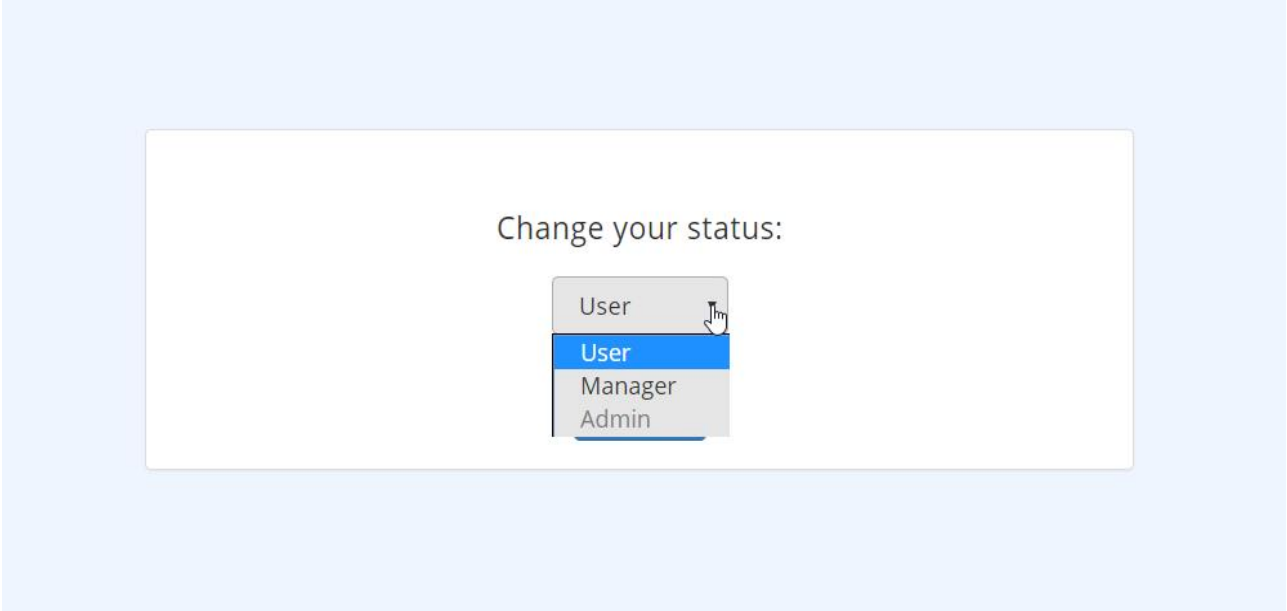

Figure 21 – Change status panel with options

One option will always be disabled and this is the current status of the user. In this example the current user is the System Administrator and a request to change status to Admin will be pointless. The user can choose between the other two options and press Confirm.

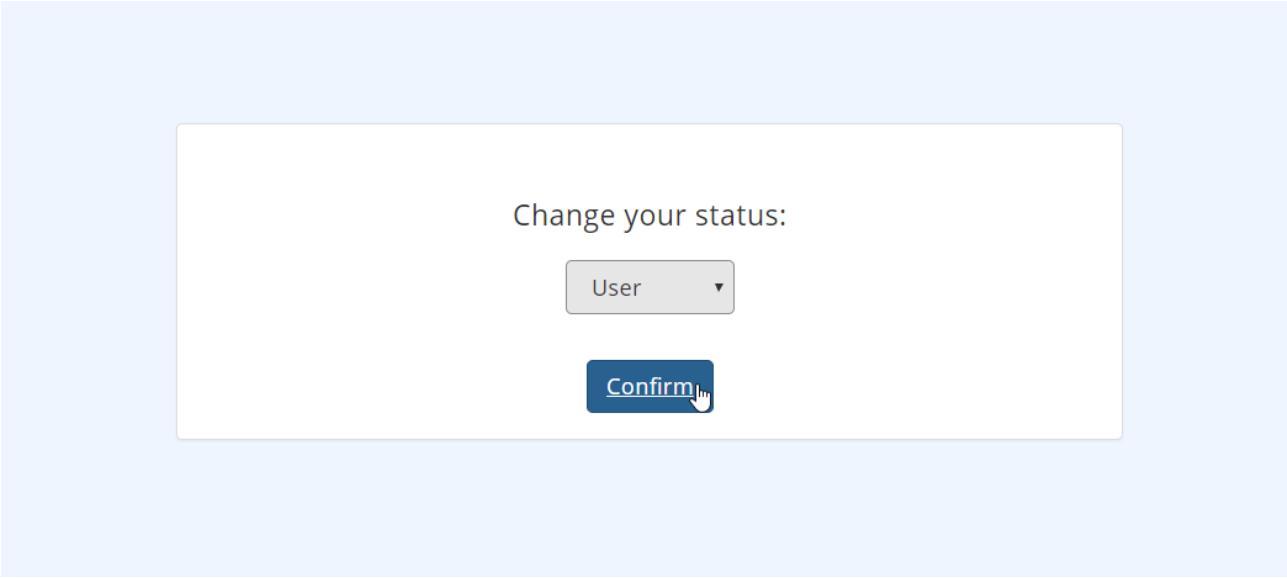

Figure 22 – Confirmation of status update request

After that the request will be sent to the System Administrator user will be redirected to their account page. It might take up to a few days for the admin to accept or decline it. A user can make as many requests as they wish, but only the last request made is going to be displayed to the administrator and only one request from a certain user can be accepted/ declined at a time.

- Depending on the current status of the user the navigation bar on the left will change. A user that has just registered to the system will have the 'User' role and will have only the basic services Privacy Enabler offers: Policies Search, Specifying preferences on private data (Questionnaire) and requesting a status change. They can also inspect the details of the compliant and non-compliant privacy policies returned from the policies search. They can't import, export and delete privacy policies, nor can they list their privacy policies uploaded to the system. They also won't be able to see other users that have made an update status request and accept/ decline it.

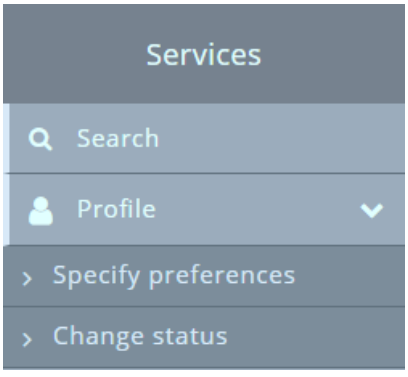

Figure 23 – User navigation bar

- A user with a Privacy Manager role will be able to import, export and delete privacy policies, as well as list their privacy policies uploaded to the system. They will also be able to use the basic services a normal user has. They won't be able to see other users that have made an update status request and accept/ decline it.

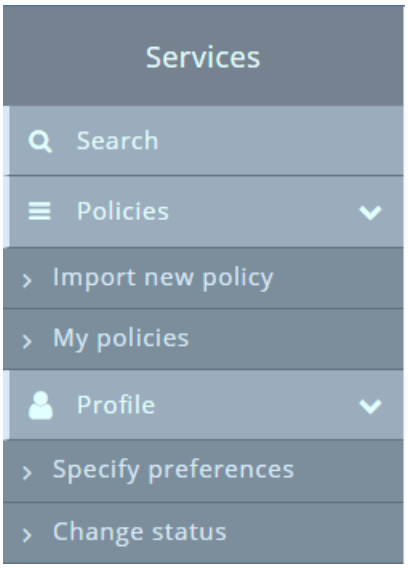

Figure 24 – Privacy Manager Navigation bar

- A user with the System Administrator role will be able to import, export and delete privacy policies, as well as list their privacy policies uploaded to the system. They will be able to see other users that have made an update status request and accept/ decline it. They will also be able to use the basic services a normal user has.

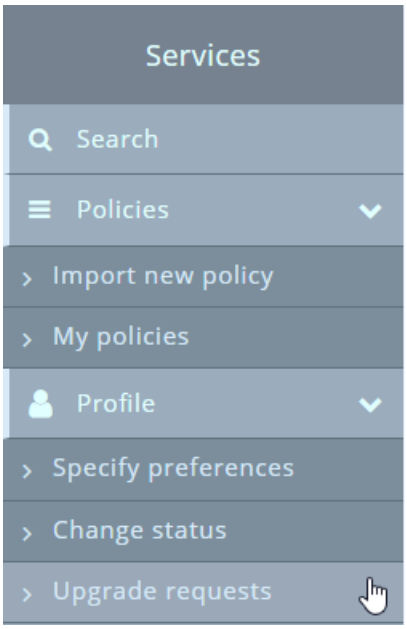

Figure 25 – Admin navigation bar

3.1.12 Upgrade Requests Page

This page will only be accessible from the system administrator. It displays the users who have made a status change request. The table shown in the panel shows the username and the requested role by the certain user. The administrator must select one user at a time and click the Accept or Decline button. The user will be removed from the table and their status will be updated if their request is accepted, or it will stay the same if their request is declined from the administrator.

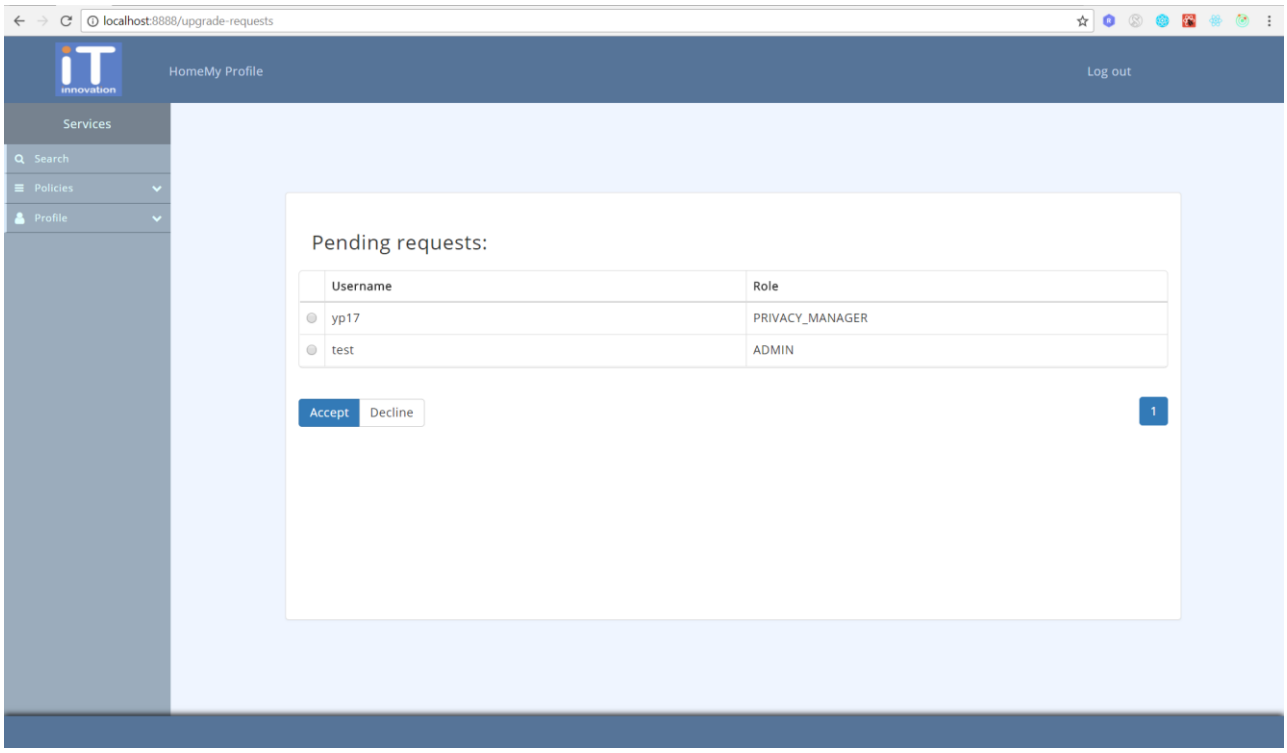

Figure 26 – Upgrade requests page

After all the users are removed from the table the administrator can return to their account page.

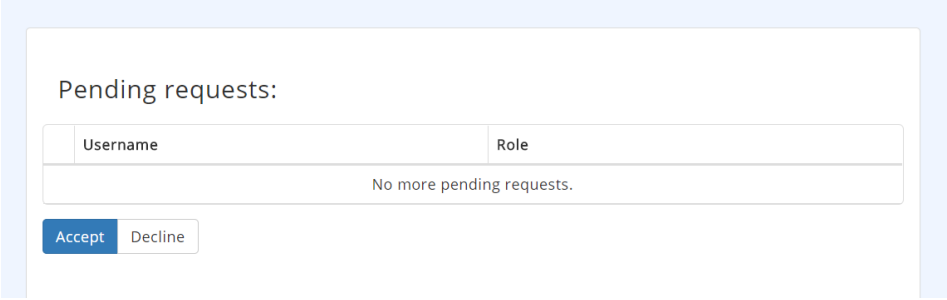

Figure 27 – No requests table

3.2 Programmer Guide

N/A

4 Unit Tests

Once the enabler has been installed and started as described in Section 2.3 the users can start testing a set of functionalities. The functionalities implement the use cases described in D3.6 [1] and are the following:

1. User registration
2. Specify privacy policy (import)
3. User's privacy preferences specification
4. Privacy aware service search

4.1 Information about Tests

The tests here provided are to be executed in the order provided since they provide to the system a set of information which are needed in the following steps. The data to be used in these tests is provided in the folder '*./server/data*' provided once the files has been unzipped.

4.2 Unit Test 1

The unit test 1 tests the user registration functionality. In order to sign up a new user click on the 'sign up' menu (see section 3.1.3) and provide full user's details:

Username: testuser

Password: testpassword

Email: test@test.com

First name: testname

Last name: testlastname

Click on 'Sign up' and check that the user is redirected to the login page (section 3.1.2). Login with the previously provided email and password:

Email: test@test.com

Password: testpassword

Check that the user is successfully logged in (see Figure 4 - Home page).

4.3 Unit Test 2

This test requires to be logged in as privacy manager user (see Table 1). Once the privacy manager user has logged in click on the 'My profile' link on the top left corner of the page and choose the action *Policies* > *Import New Policy* as shown in Figure 24.

Click on the 'Drag and drop' area as depicted in Figure 12 and choose the policy file 'automotive1.ttl' from the folder '*./server/data/policies*'.

Provide 'automotive1' as name and click on the "import policy" button.

Click on *Policies* > *My Policies* link on the menu on the left and ascertain that the policy has been successfully imported.

4.4 Unit Test 3

This test requires to be logged in as normal user (see Table 1). Once the user has logged in click on the 'My profile' link on the top left corner of the page and choose the action *Profile* > *Specify Preferences* as shown in Figure 23.

Click on the link "*Start Questionnaire*" (see Figure 17) and provide different levels of concern to different action types provided. Click 'Submit' once the questionnaire has completed.

4.5 Unit Test 4

This test requires that all policies contained in the 'server/data/policies' folder to be imported in the system and to be logged in as normal user (see Table 1). Once the user has logged in click on the 'My profile' link on the top left corner of the page and choose the action *Search* as shown in Figure 23.

Move the slider to specify different privacy profile levels of the users (from totally unconcerned to pragmatist) (see Figure 9) and see that the privacy policy results change accordingly.

5 Abbreviations

5G-PPP	5G Infrastructure Public Private Partnership

6 References

[1] Deliverable D3.6. 5G-PPP security enablers open specifications (v2.0)..