SUCCESS

M4.3: Successful Pilot 2

Grant Agreement:	N/A
Project Acronym:	SUCCESS
Project Name:	SecUre aCCESSibility for the internet of things
Instrument:	CHIST-ERA Call 2015
Thematic Priority:	SPTIoT
Start Date:	1 December 2016
Duration:	36 months
Document Type[1]:	T (Technical Report)
Document Distribution[2]:	CO (Confidential)
Document Code[3]:	SUCCESS-MU-PR-001
Version:	v1.0
Editor (Partner):	J. Gimenez (MU)
Contributors:	J. Augusto, J. Gimenez, F. Kammüller
Workpackage(s):	WP4
Reviewer(s):	F. Kammüller (MU)
Due Date:	Month 35
Submission Date:	Oct 2019
Number of Pages:	11

Funded by EPSRC Engineering and Physical Sciences Research Council, Agence Nationale de la Recherche ANR, NWO Netherlands Organisation for Scientific Research

[1] MD = management document; TR = technical report; D = deliverable; P = published paper; CD = communication/dissemination.
[2] PU = Public; PP = Restricted to other programme participants (including the Commission Services); RE = Restricted to a group specified by the consortium (including the Commission Services); CO = Confidential, only for members of the consortium (including the Commission Services).

[3] This code is constructed as described in the H2020 Project Handbook.

M4.3: Successful Pilot 2

J. Gimenez[1]

[1]MU

REVISION HISTORY

Date	Version	Author	Modification
10.12.2019	1.0	F. Kammüller	Started the document
27.1.2020	1.	F. Kammüller	Approval

APPROVALS

Role	Name	Partner	Date
Project Manager	F. Kammüller	MU	27.1.2020

Contents

1 Executive Summary

This is the documentation of the successful Pilot 1. An earlier first draft of this has has been provided in Milestone M7 (M4.2).

2 Tool Set

2.1 The server cloud

The server has been installed and deployed using the 000webhost.com site provided by Hostinger refPAGE. This platform gives enough features to cover the pilot specifications and to deploy it. There is not a Domain name since that depending on each customer. The URL to access to the public part is:

https://pilot2.000webhostapp.com

The users created to test and browse are:

- user:testpu@mdx.ac.uk - password: passwordpu
- user:testsu@mdx.ac.uk - password: passwordsu

These two users have been associated with some content to test the navigation and design behaviour.

2.2 Graphic user interface: web page

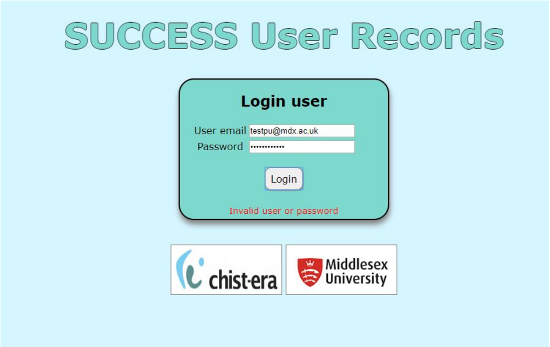
The GUI has been developed using HTML5, CSS and JavaScript(JS). JQUERY is the JS library used to manage the HTML content and no special JS frameworks have been used from the front-end logic. This decision bases on creating a simple GUI which is not going to increase its complexity. The design is basic to provide an easier user's understanding and experience of the platform and providing meaningful information extract from requirements.

The structure of the interface does not follow any Model-View-Controler (MVC) patter. The load of the information management is carried out by the client browser. The main reasons to take this application design has been:

- The complex of the application is not high enough in the number of resources to create a complex structure MVC. It also does not expect a growth in the structure, models or functionalities according to the requirements.
- JS script has better performance and is faster than PHP. Since the server could have a low performance (actually that current test server has, since that is a free hosting) and the quantity of information to generate by the query is not to heavy by not exists photos or other heavy content. It avoids the server overloads generating HTML content in case many users are requesting and leaves this labour to the browsers.

2.3 Login screen

The GUI includes an initial login screen which depending on the user logged, the system determines the user's role allowing him/her to access different resources, options and elements. The login screen also includes a ”red” message that shows when the server returns an error related to incorrect user or password, IP block and so on. In another case, the application redirects the user to the main page.



SUCCESS User Records

Login user

User email testpu@mdx.ac.uk

Password ••••••••••••

Invalid user or password

Figure 2.1: Login screen with error message.

2.4 Web Content

The page has been designed simply to allow easy access and understanding of the information to show. Thereby the menu options offer the basic actions proposed initially, identically to Android App described in D4.1: Pilot 1 Documentation.

The menu options offer access to the resources that are able to check according to the user's role. Since the security is managed by the server, the GUI can request information without limitations at the client level since is the server which response to the requests depending on the user's role and access granted. O course, as it was explained in D4.1, the server blocks the IP after 3 login attempts.

Each menu option shows the list of elements related to it. The rows can be expanded if there is more useful information in other case showing the row with the content is enough. Each row also includes buttons as actions regard to the resource and the state of the element shown in the row. E.g.: an Access element which was revoked cannot be revoked again, so this button is hidden.

- **Outcomes**

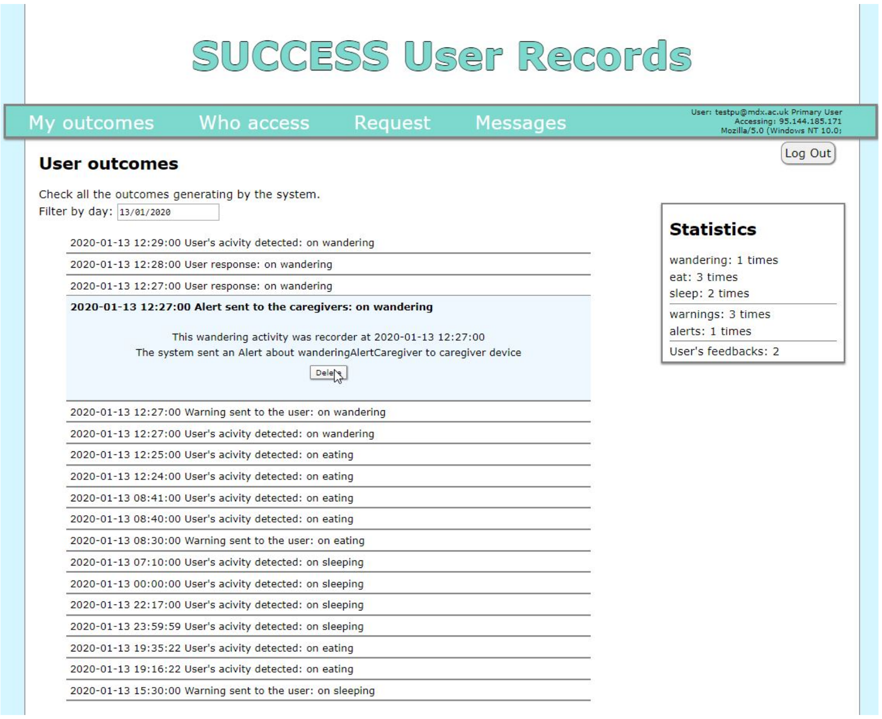
  A primary user can see just his results, whilst other user's roles can choose the user to check the records. The figure 2.2 shows this screen.

  The records can be filtered by day to show more precise information. It also loads a small square with statistics in the day selected. The option to show graphs is leaving for futures requirements from stakeholders who can decide what could be the best way to understand the information.

  Each row shows the date and the generic subject. When it clicks on the row, it is rolled out showing more details about the entry. By the moment, the information is related to the activities detected in the house, the warnings to the users, alerts to caregivers and information from the user such as the "mood quiz" and user's responses to the system when that alerts him. This last option can be extended with other bio-sensors such as heart-rate, blood pressure, etc.

  The information shows the date and time when the activity happens, the name of the activity and the context related to it.

- **Requests for access** This option appears in both roles. This list shows all requests as a history with the date, the user to/from request (whether is primary or other users) and the



SUCCESS User Records

User: testpu@mdx.ac.uk Primary User
Accessing: 95.144.185.171
Mozilla/5.0 (Windows NT 10.0;

User outcomes

Check all the outcomes generating by the system.
Filter by day: 13/01/2020

```
2020-01-13 12:29:00 User's acivity detected: on wandering
2020-01-13 12:28:00 User response: on wandering
2020-01-13 12:27:00 User response: on wandering
2020-01-13 12:27:00 Alert sent to the caregivers: on wandering

        This wandering activity was recorder at 2020-01-13 12:27:00
  The system sent an Alert about wanderingAlertCaregiver to caregiver device

2020-01-13 12:27:00 Warning sent to the user: on wandering
2020-01-13 12:27:00 User's acivity detected: on wandering
2020-01-13 12:25:00 User's acivity detected: on eating
2020-01-13 12:24:00 User's acivity detected: on eating
2020-01-13 08:41:00 User's acivity detected: on eating
2020-01-13 08:40:00 User's acivity detected: on eating
2020-01-13 08:30:00 Warning sent to the user: on eating
2020-01-13 07:10:00 User's acivity detected: on sleeping
2020-01-13 00:00:00 User's acivity detected: on sleeping
2020-01-13 22:17:00 User's acivity detected: on sleeping
2020-01-13 23:59:59 User's acivity detected: on sleeping
2020-01-13 19:35:22 User's acivity detected: on eating
2020-01-13 19:16:22 User's acivity detected: on eating
2020-01-13 15:30:00 Warning sent to the user: on sleeping
```

Statistics

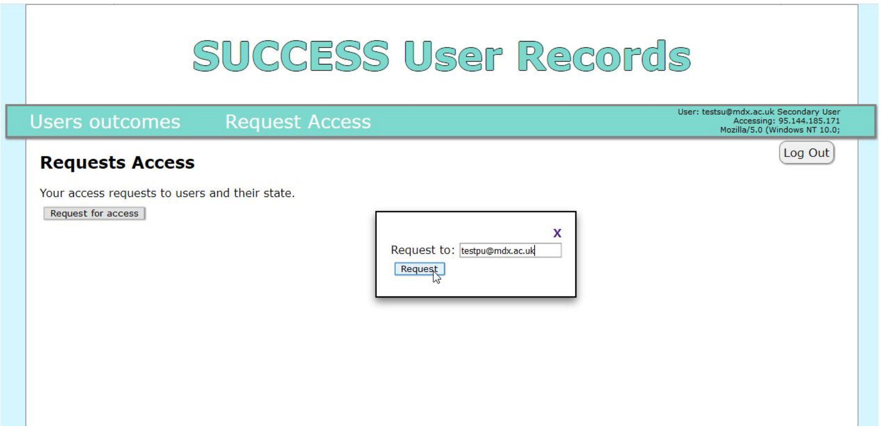
wandering: 1 times
eat: 3 times
sleep: 2 times

warnings: 3 times
alerts: 1 times

User's feedbacks: 2

Figure 2.2: Outcomes list screen.

state of the request (pending, accepted, denied). PUs can see the buttons to accept or deny the request which upgrades the state for the user who asks for. The figure 2.3 shows a SU screen to request for access to a PU. The PU can check in his Request tab the request 2.4.



SUCCESS User Records

User: testsu@mdx.ac.uk Secondary User
Accessing: 95.144.185.171
Mozilla/5.0 (Windows NT 10.0;

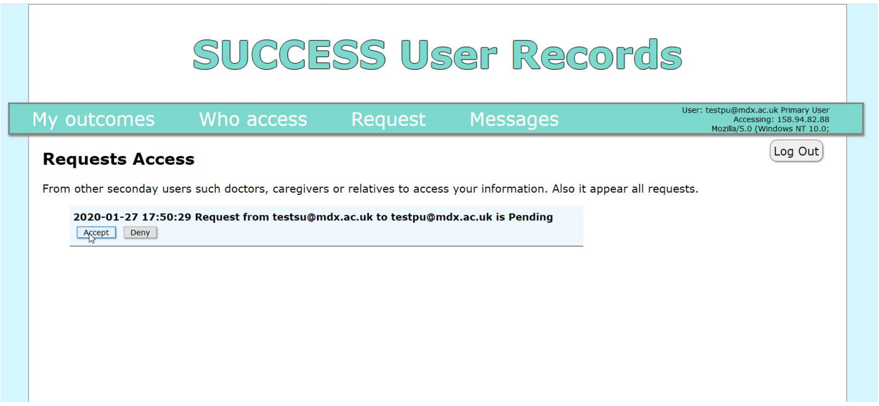
Requests Access

Your access requests to users and their state.

Request to: testpu@mdx.ac.uk

Figure 2.3: Secondary user requesting for access to testpu user.

- **Access** Primary users (PS) are the one which sees this option. Here the user can check what other users can see his/her information. From here the user can revoke the access to a user using the button ”revoke”. Figure 2.5 presents the screen where the user can manage the access by revoking.
- **Messages** This list shows the messages generated by server related to security such as a



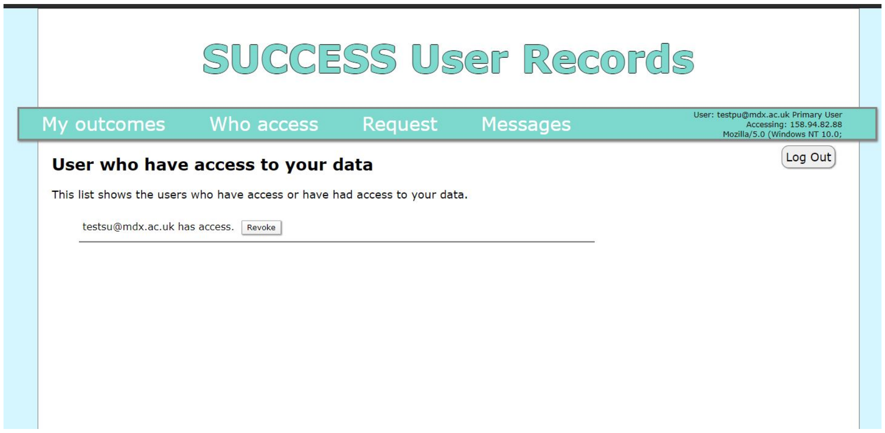
User: testpu@mdx.ac.uk Primary User
Accessing: 158.94.82.88
Mozilla/5.0 (Windows NT 10.0;

Requests Access

From other seconday users such doctors, caregivers or relatives to access your information. Also it appear all requests.

2020-01-27 17:50:29 Request from testsu@mdx.ac.uk to testpu@mdx.ac.uk is Pending

Figure 2.4: Primary user accepting the request.



User: testpu@mdx.ac.uk Primary User
Accessing: 158.94.82.88
Mozilla/5.0 (Windows NT 10.0;

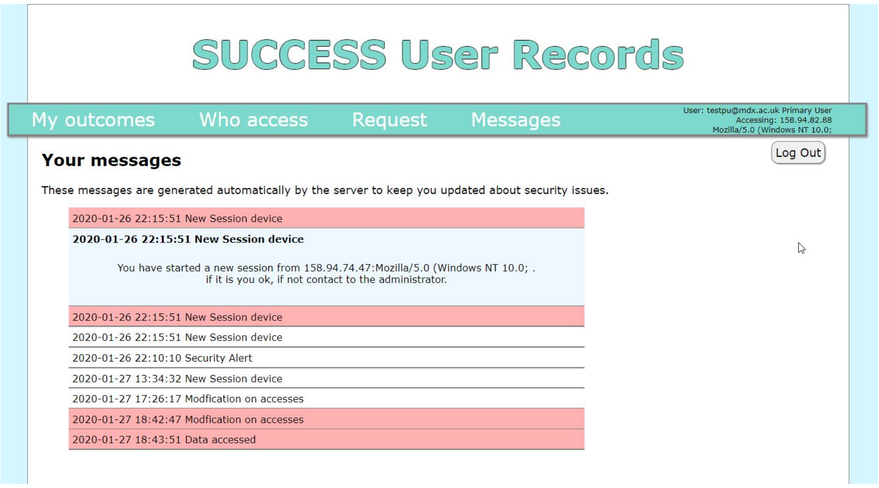
User who have access to your data

This list shows the users who have access or have had access to your data.

testsu@mdx.ac.uk has access.

Figure 2.5: Once the request was accepted the PU can revoke the access to the user.

login in a primary user account from a new IP, whether an IP has been blocked, whether a user has accessed to the PU data and when there are modifications in users' access. When it clicks in a row, it expands and the message change to read status automatically. Notice that the messages unread appear in red. Non-PUs do not have this option. Figure 2.6 shows a screen shot of PU messages screen.



User: testpu@mdx.ac.uk Primary User
Accessing: 158.94.82.88
Mozilla/5.0 (Windows NT 10.0;

Your messages

These messages are generated automatically by the server to keep you updated about security issues.

2020-01-26 22:15:51 New Session device

2020-01-26 22:15:51 New Session device

You have started a new session from 158.94.74.47:Mozilla/5.0 (Windows NT 10.0; .
if it is you ok, if not contact to the administrator.

2020-01-26 22:15:51 New Session device
2020-01-26 22:15:51 New Session device
2020-01-26 22:10:10 Security Alert
2020-01-27 13:34:32 New Session device
2020-01-27 17:26:17 Modfication on accesses
2020-01-27 18:42:47 Modfication on accesses
2020-01-27 18:43:51 Data accessed

Figure 2.6: Messages screen.

The GUI also shows at the top right page corner the logout button and the user's information such as account name, IP and browser version of the current session.

2.5 GUI migration issues

Since we do not have a full control over the server configuration as we have in the lab, some modifications have had to included in the back-end. There are specific PHP files adapted to this sever to cover issues related to server. For example, the Ajax request to modify using PUT methods generates a recognize and not solved problems documented. The causes are unknown, so meanwhile this php files solve the problem Again, as the server controls the security based on the session and the user id and role, this new files do not represent a security lack.

3 Conclusion

Pilot 2 has been deployed and tested in an external server simulating the end final environment. It is ready to test in a real external environment such as users' homes, hospitals, etc.

There are still some technical features or requirements which depend on each environment centre wherein the application is installed such as the SSL certificate or rules according to the company requirement.

Bibliography