Suzanna Wentzel - s1850512
Jesper Simon - s1820338
Chris Witteveen - s1847821
Milo Cesar - s1829688
Danique Lummen - s1853155
Apostolis Christoulias - s1833383

Requirements Specification for Door Authorization in Care Centre “Liemerije”

27 October 2016

1. Introduction

In a lot of care centres, the way the clients get to different rooms is by asking a person of the nursing staff to open doors for them. This because most of the time only the nursing staff have keys because giving everyone physical keys to each room would both be very expensive and bring lots of extra problems with people losing keys etc.

Care Centre “Liemerije” intends to replace this rather inconvenient practice with an entirely new keycard system. This system issues a keycard to every client (the care centre prefers to speak of “clients”, rather than “patients”) and member of the nursing staff. These keycards will replace the ‘normal’ keys that are used now, and are personalized so that only doors that the person has access to will be opened, doors to which they do not have access will stay closed. This means that it is less likely for clients to get lost in the big building since they can only open a specific set of doors and thus won’t leave the space they know and where they live. Next to this the procedure of giving someone a new card because their old one got lost or is broken is much more simple, instead of having a locksmith create an entire new set of keys, we simply assign a new keycard to the person.

There are multiple advantages to this new system, the amount of work needed for a lost or broken key is a lot less, as stated before. The system is also a lot more secure, this because the new system will use public/private key encryption, which makes it hard for cards to be hacked or doors to be opened when they should not.

This system will not eliminate all problems, there will still be problems with persons losing their keys and trying to get into rooms which they do not have access to. However, the system will still improve the working conditions in the care centre.

2. Important stakeholders

Client: Care Centre “Liemerije”
Contact Person: Harold Koerntjes, team manager.

Developer: TCS Project Group 19
Contact Person: Suzanna Wentzel, developer.

Operational management: Liemerije

End users: Nursing staff and clients.

3. Mission statement

Motivation:
At care center Liemerije, access is given through the usage of keys. This manner of access is however become inconvenient and outdated, with in mind that every door needs a different key. This has become such a problem that a security system must be implemented. This security measure will replace the outdated keys by one personal key card which allows access to authorized areas. There is also the problem of unauthorized entering or leave of the building, which would also be prevented by the implementation of the key card system.

Type of system:
The system will consist of several key cards and scanners, which will use a database with authorization data of staff and clients.

Goal of the system:
The system allows staff and clients of the care center to access certain areas they are authorised to enter. This heightens the security of the staff and especially the clients.

Exclusions:
The system can allow and deny access to different facilities to different staff and clients. The security between the card and the card-reader is limited, because we cannot control the chip in the card.

Approach:
The system access will be based upon two aspects: frequent access of a certain area and the status of a person.

4. Constraints, assumptions, definitions

4.1 Constraints

- The system has to be Arduino based.
- The tags used must be MIFARE cards with a size of at least 1 kB.
- The preliminary system should be operational by the end of 2-11-2016
- The system should be fully operational by the end of 4-11-2016

4.2 Assumptions

The data exchange between the keycard and the reader can not be secured, since the controller of the card is inaccessible. Therefore it is assumed that the communication between these two instances is secure.

4.3 Definitions

UID - Unique Identifier. Each keycard has its own unique number by which it can be recognized. These UIDs are used to check if a certain person has access to a certain door.

RFID tag - A RFID tag uses electromagnetic fields to automatically identify and track tags attached to objects. These tags contain electronically stored information. They can be attached to almost everything, and in the case of this this system: keycards.

5. Functional requirements

The functional requirements for this project are written in the form of user stories and are sorted by using the MoSCoW method, which sorts the user stories according to priority: Must, Should, Could and Won't.

Must

As a nurse I want to get into the rooms of all my clients

- Test with door to which the nurse has access (pass)
- Test with door to which the nurse has no access (fail)

As a nurse I want to get into the common areas

- Test with door to which the nurse has access (pass)
- Test with door to which the nurse has no access (fail)

As a nurse I want to get into the nurse-only areas

- Test with door to which the nurse has access (pass)
- Test with door to which the nurse has no access (fail)

As a client I want to get into my own room

- Test with door for the clients own room (pass)
- Test with door for another client's room (fail)
- Test with door for a door which the client used to own (fail)

As a client I want to get into the common areas

- Test with door to which the client has access (pass)
- Test with door to which the client has no access (fail)

As a doctor I want to get into all the rooms

- Test with door to which doctor has access (pass)

As a system administrator I don't want old 'cards' to be able to enter the rooms

- Test with door with a card that belongs to an old client/staff member (door should stay closed) (pass)
- Test with door with a card that belongs to a current client/staff member on a door he/she has access to (door should open) (fail)

As a system administrator I want to be able to issue a new 'card'

- Test with an old card (fail)
- Test with a new card without access (pass)

As a system administrator I want to be able to disable a 'card' (temporarily)

- Test with an enabled card (pass)
- Test with a disabled card (false)

As a system administrator I want the UID of an RFID-tag to be sent securely between the arduino and the computer

As a system administrator I want to be able to compare the UID of an RFID-tag with the saved UIDs in a database to check whether it is authorized or not.

- Test with a door with an authorized UID (pass)
- Test with a door with an non-authorized UID (fail)

As a system administrator I want to be able to save the UID of a RFID-tag in the database.

- Test with UID that's not yet in the database (pass)
- Test with UID that is already in the database (fail)

As a system administrator I want to be able to delete the UID of a RFID-tag from the database.

- Test with UID that's not yet in the database (fail)
- Test with UID that is already in the database (pass)

As a system administrator I want no users to be able to copy or see the authorized UID of a RFID-tag

As a user I want the doors to open within 3 seconds of scanning my card

- Test with doors opening after 1 second (pass)
- Test with doors opening after 4 seconds (fail)

- Test with doors not opening (fail)

Should

As a user I want visual or audible feedback when my card has been scanned

- Test with a key for the scanner and hear a noise or see a light (pass)
- Test with a key and gain no feedback (fail)

As a user I want visual or audible feedback regarding my authorization status

- Test on an door and hear or see something (pass)
- Test on an unauthorized door and hear or see nothing (fail)

Could

As a system administrator I want to revoke all access to a door

As a team manager I want to be able to control the authorization of all cards and doors belongs to my team

Won't

As a team manager I want to see who opened which door at what time

As a team manager I want to see who is authorized to open a specific door

As a team manager I want to see how many cards are authorized at any given time

As a system administrator I want to authorize keys of visitors

As a visitor I want to have access to the common areas during visitor hours

- Test being able to enter the common area (pass)
- Test not being able to enter the common area (fail)

As a client I want to (temporarily) authorize specific cards which belong to my family members

As a system administrator I want to open all the doors at any time in case of an emergency

Appendices

Appendix A - Interview:

We asked a nurse in a nursing home for elderly people some question regarding the entering of buildings and rooms with a digital “key”. These are the questions we asked and discussed:

Would you as a member of the staff and your clients benefit from a digital wireless key system?

It would benefit us both, most of the elderly are not able to quickly grab a key and put it in the keyhole anymore, the tags that could be used in a wireless system are easier to wear as let’s say a necklace and they are easier to hold in front of a scanner. For us it would be easier because we only need one key which can be changed “on the fly”

Would it be beneficial for the clients to have their own key to be able to enter the common areas and their own room?

While our own clients have an “open” style of common areas (they can just walk in and out as they please) so it is never locked, but I could see that it would be easier for them to enter these areas if they would be closed. In our own nursing home we would use these new keys to let clients enter the building on their own, currently only staff can open those doors from the outside, of somebody needs to open it from the inside.

Are there any areas closed for the clients?

At night most of the common areas are closed down, we also have an office for the nurses to which only the staff has access. We also have medicine lockers which are closed for the clients.

Could you put the following aspects in order of importance.

- Security (Only access the required rooms)
- Speed (Don’t wait too long for a door to open)
- Ease of Use (Everybody should understand the system and be able to use it)

I can’t tell you whether security or ease of use is more important since both of them need to function 100% correctly. If nobody understands the system it is of no use and if there is a security flaw the system should clearly not be used. Security of our clients is one of our most important topics. The speed is of course important, we should not be annoyed by the time we have the door opened but it currently takes a long time for us to find the keys and open the doors so that shouldn’t be too much of a problem.

This Interview led to a couple of changes in our requirements; in order of adding requirements, we added the aspect of the speed at which the doors open when you scan the

card. This interview also led to some changes in the priority from some requirements. The aspects of security are placed high in the ranking (mostly in Must).

Appendix B - Mock up of system

Arduino:

- A ‘door’ ID
- The server’s Public Key
- A custom Public/Private key pair

Server:

- The public keys of all arduinos, which are stored in the database.
- A custom Public/Private key pair
- A database with the hashed UIDs of the cards and the doors to which they have access.

Key:

- A custom UID

Implementation:

Arduino side:

1. The arduino reads a key and gets it UID
2. The arduino makes a value key pair with its own door ID and the read UID
3. The arduino encrypts this value key pair using the servers public key
4. The arduino sends this now secured value key pair to the server

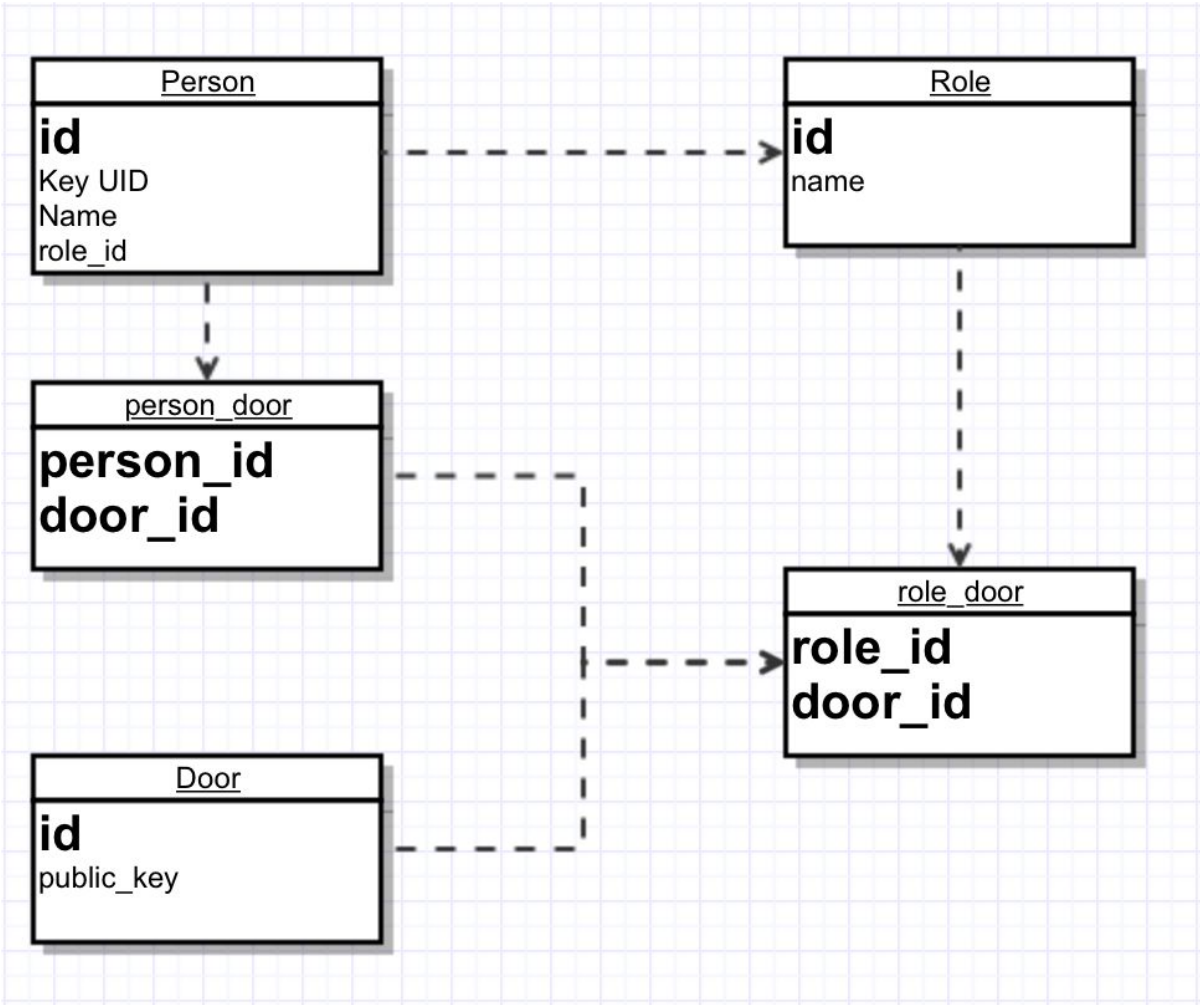
Server side:

1. The server uses its private key to decrypt the value key pair
2. The server hashes the UID
3. The server compares the hashed UID with the stored UIDs in the database and gets the authorization status of the key
4. The server creates a value key pair with the key UID and a boolean value indicating the authorization status
5. The server uses the public key of the arduino to encrypt the new value key pair
6. The server sends this now secured value key pair back to the original arduino

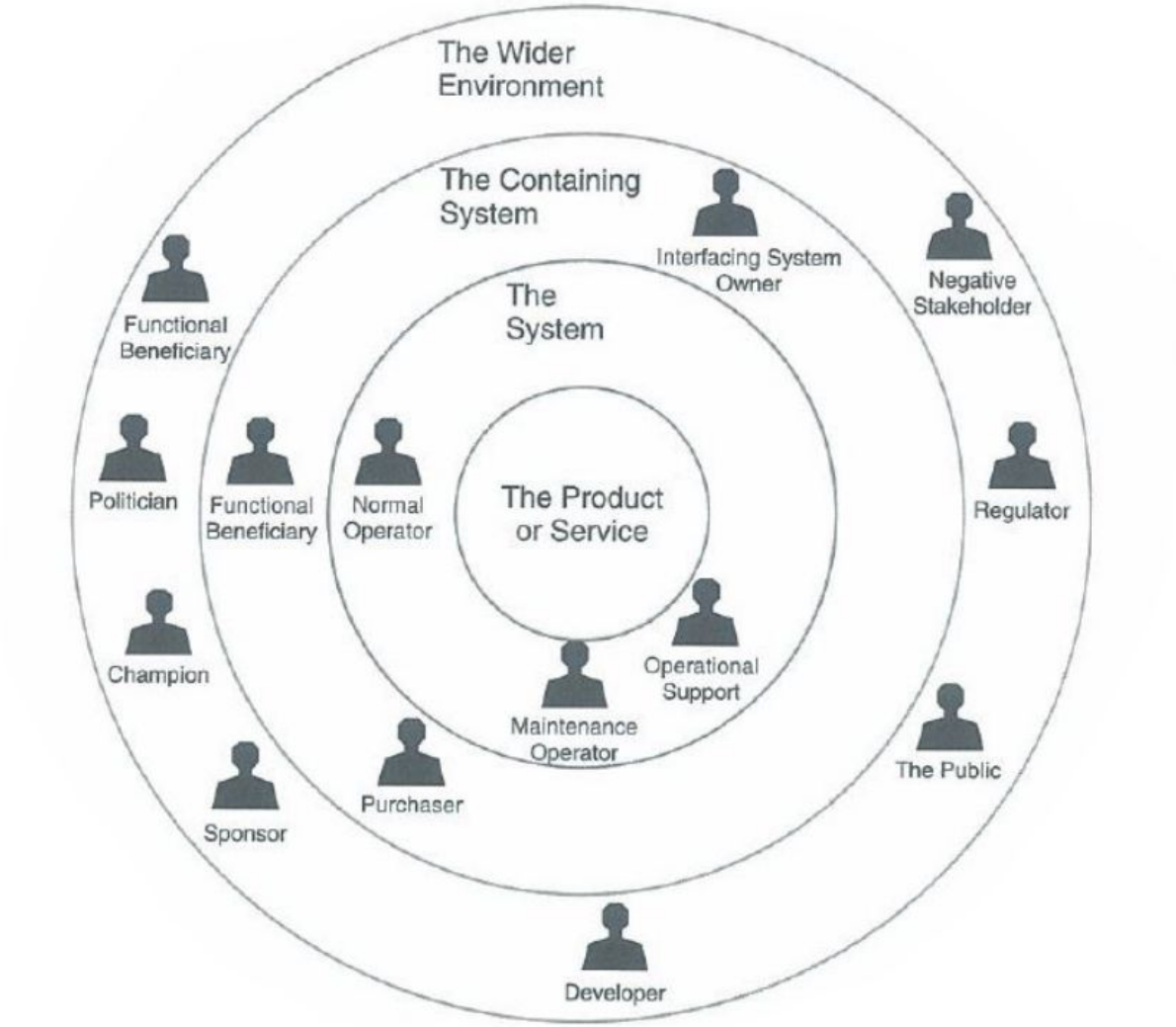
Arduino side:

1. The arduino uses its private key to decrypt the value key pair
2. The arduino checks if the original send UID is equal to the UID it has just gotten back.
3. The arduino handles in regards to the boolean value stored in the value key pair.

Database design:



Appendix C: Stakeholder analysis



In this project, a couple of stakeholders are involved. Some of them belong in the system scale (as can be seen in the image above.) One of these stakeholders is a company that will make sure the system will be maintained; which will be the TCS group 19. These would be the maintenance operators. The operational support would be handed over to the helpdesk at the Care centre Liemerije

Others belong to the containing system. These stakeholders are for example people who benefit from the function. These people will be the nurses at Liemerije, they will be able to get in the rooms faster, and it will cause less problems with clients for them. They are not the only functional beneficiaries, there are also the Clients themselves. They will have less trouble using keys, because now they can use the tags.

The last stakeholders belong to the wider environment, that will be the care centre itself, and the developers and the negative stakeholders (competitive companies who would want to build and implement this security system themselves, or people who would want it the old-fashioned way).