Unsolvable Solutions

Client: CSIR DSSR

Architecturall Requirements

Eavesdropping Protection in Conclave

Members:	*Student Number:*
Edwin Fullard	12048675
Jaco Bezuidenhoudt	11013878
Jandre Coetzee	10693077
Maret Stoffberg	11071762
Ryno Pierce	12003922

Contents

1 Access and Itegration Requirements

1.1 Human Access Channels

1.1.1 Via Web Browser

The user must be able to access the data from the server these standard web browser: Mozilla Firefox, Google Chrome and Microsoft Internet Explorer. It must have a user friendly GUI.

1.1.2 Via Android device

This device is used for the malware as well as the protection software.

1.1.3 Via NFC Nodes and an Edison

This is used outside the meeting for the access control and the protection application.

1.2 System Access Channels

1.3 Integration Access Channels

2 Quality Requirements

2.1 Scalability

2.1.1 EPIC

the server must be able to handle a large amount of users and users must be able to use the system simultaneously. However, the controlled access to a meeting, via the Gateway and the Node will only have a limit of one gateway per meeting and at most three nodes per meeting.

2.1.2 Malware

The server can only handle one live stream recording at a time.

2.2 Performance Requirements

The system does not have specific performance requirements, but the application to gateway operations should respond within less than 1 second, because it may delay the meeting unnecessarily. The server query operations may process up to 5 seconds long.

2.3 Maintainability

The system must be easily maintainable. The application and server may be updated in time, to fit the latest technologies.

2.4 Reliability and Availability

The application must be available from the Google play store, and the access to the web server can be found online at projectepic.info.

2.5 Auditability

The system log the entrance and exit of all meetings. For each meeting the log contains the users allowed, the users that attended, their entrance and exit times as well as the initial time and place of the meeting.

2.6 Security

The NFC components should not be hackable.

2.7 Monitorability

The response of the Nodes is visible with the LED light showing the permission.

2.8 Testability

All the components must be tested separate at first, unit testing, and after completion the whole system must be tested.
For each service the pre and post conditios must be met.

2.9 Usability

All the components must be intuitive and easy to use. Any user that is Android literate and computer literate must be able to use the system. The physical components must be labelled accordingly.
The User Manual may be used for more information on any of the components.

2.10 Integrability

The different components of the system should work together and the system must also be able to handle future additions to it.

3 Architecture constraints

4 Technologies Used

- NFC
- NodeJS
- Arduino
- MongoDB
- Passport
- Java
- Android SDK
- TCP
- UDP