1. Access and integration requirements:
   1. Human access channels
      1. From a web browser
         1. 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.
      2. From an Android device
         1. This device is used for the malware as well as the protection software.
      3. From an Edison and NFC Nodes
         1. This is used outside the meeting for the access control and the protection application.
   2. System access channels
   3. Integration channels
2. Quality requirements
   1. Scalability
      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 gateway node will only have a limit of one gateway per meeting and at most three nodes per meeting.
      2. Malware: the user only handles one live stream recording at a time.
   2. Performance requirements
      1. 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 4 seconds long.
   3. Maintainability
      1. The system must be easy to maintain. If the device is physically damaged, it should be replaced and the software should be reinstalled. Server must be restartable
   4. Reliability and availability
   5. Auditability
      1. 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.
   6. Security
   7. Monitorability
   8. Testability
      1. Unit test the different components separate and integration testing of the components assembled.
      2. For each service the pre and post conditions must be met.
   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.

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

1. Architecture constraints
2. Technologies
   1. NFC
   2. NodeJS
   3. Arduino
   4. MongoDB
   5. Passport
   6. Java
   7. AndroidSDK
   8. TCP
   9. UDP

////

\subsection{Human Access Channels}

\subsection{System Access Channels}

\subsection{Integration Access Channels}

\newpage

\section{Quality Requirements}

\subsection{Scalability}

\subsection{Performance requirements

\subsection{Maintainability}

\subsection{reliability and Availability

\subsection{Auditability}

\subsection{Security}

\subsection{Monitorability}

\subsection{Testability}

\subsection{Usability}

\subsection{Integrability}

\newpage

\section{Architecture constraints}

\section{Technologies Used}

\begin{itemise}

\item NFC

\item NodeJS

\item Arduino

\item MongoDB

\item Passport

\item Java

\item Android SDK

\item TCP

\item UDP

\end{itemise}

Architectural patterns

Layering

Each separate part of the system use the layering concept one way or another.

1. The server: The server uses