Non-functional requirements

Performance requirements

The system has to guarantee a good level of usability.   
The response time is closed to zero, so the performances are strictly related to the speed of user’s internet connection.  
The connection between the system and the embedded taxi device is made by UMTS technology: all the LargeCity jurisdiction is covered by UMTS signal so it guarantee a very fast connection.

Design constraint

The server side and web application will be developed in Java2EE, they will inherit all language constraints. Will be used Java language For android devices and Swift language for Apple devices.

Software system attributes

MTS System has to be reachable anytime 24 h/24 7 days / 7. To achieve this goal is necessary to use a dedicated server hosted by professional data center company. This exempt Municipality to buy and maintain the server and its infrastructures and it also offers improvements in terms of security, backup of data and availability of the system.  
This solution is also good in terms of scalability, in case the system enlarge its traffic is possible to switch up to more power hardware without big outgoings.

In terms of maintainability, due to the integration of some API (as assert in point xx), all the application code has to be well documented.

Security

User-side

MTS system implements a login authentication to protect the info of the user.   
The authentication login asks to user the email address and the password, random generated by the system and send by SMS to him after the registration.  
User’s password are saved using a hashing mechanism. After the first login, user is allowed to change his password. The password length has to be at least 8, including at least one number and one capital letter. Non special character are allowed.

To prevent hacking action after 3 attempts the system, in addition to email and password, requires captcha test and after the fifth attempt block the user for one day.

Application-side

On the application side, the system has to prevent any kind of sql injection attack.

System use HTTP protocol to communicate with user and driver. It might be better use the HTTPS protocol, to improve security. This solution could be more expensive.

Driver-side

The device given to driver requires login to work. Login require a id of driver and a password random generated by the system. Id and password are given by the administrator and the password could be regenerate by the system (this action is done by the admin).

Administrator-side

Administrator can access to his interface through a login that requires a password given by the developers and it cannot be modified.

Hardware interfaces

The MTS System has to communicate via internet and via SMS message.

For this reason the server that hold the system must have a network interface that allows TCP communication protocol and a integrated board that support at least the GSM technology.

For the SMS communication, instead of hardware interface it could be possible to use a external web service that allow this.