Peer review of "authentication methods"

This is a peer review of a report that is currently under development, and therefore, there will be parts of the project, that will not be in this review. An approach to the problem and a demarcation of the project ought to be ready. Let it be said, that it seems like this is a ambitious and exciting project, with an interessting and important theme, that is highly relevant these days. The group has chosen an analytical approach of existing systems, before development of a new system.

The approach to the problem is clear and concise.: If security on (mobile divices), is on a level high enough to provide adequate support for them or they can provide more threats and problems to users than benefits.

As it is mentioned, the potential for mobile services is very wide, and the examples they have is: mobile health systems, mobile banking and mobile learning. To solve the problem the group have a few questions they want to address through the work with the project, two of the questions are:

- What are most common and accepted authentication methods for mobile services?

- How do people accept them and what are their opinions regarding security on mobile device?

There is a possibility, that the theme and measurement in the project is to wide. Sometimes these have to be delimited, and there must be developed a sufficient exploratorydesign, which is the frame for the methodical policy. It is often that we do not want the search results to be to wide, ever since the search results is related to the theme of the project. The group have, on the other hand, solved this matter in a good way. The first phase of the project is done, where they did research on what is already developed and available in the area of user authentication for mobile service. For this part the group have actively used internet and databases, which is recomended. It is generally concluded that the field is very wide, with a massieve amount of search result, they have therefore organized the findings in four groups:

- Authentication methods based on something that user know
- Authentication methods based on something that user has
- Authentication methods based on something that user is
- Authentication methods based on user location

The document is diveded in sections, covering the groups above, and each group covering four main topics: Implementation for stationary devices, Implementation for mobile devices, security level that is provided, and usability issues. Beside theory, which is background information on what already exists, the group also want to gain knowledge about users and their acceptance of authentication methods on mobile devices. The group have created questionnaires, which will identify main requirements and satisfaction with different user authentication methods, and generally find out what is good or bad with the mobile service. As mentioned, the group has chosen an analytical approach of existing systems. It is therefore of high importance, to have a well working system for collection and analysis of the data. Above all ever since the group are using more than one method, this is a possibility for generalizations, and to find evidence for the final reult. The time for discussion of the theme is also of high importance. This will help the group not to draw any quick conclusions,

something that often ends in bad conclusions. It is important to collect all of the information, and analyze this in a good way. It is mentioned the document that this is something the group have taken notice of, and will do in the future work.

The questionnaires the group wish to use in future work looks nice. The group has included relevant questions, and the target group are between ages of 18 og 40 years, it is also great that the questions are not to personal. They have described what they want to find out, and what is of importance to know. Table 1: “Characteristics of different security methods” is well made. It has a summary of the results for the different methodes. This way the group has a overview of the methodes that has been analyzed, and the weakness and strength for each method.

Generaly it seems like they have good overview of the project, and know what they want. Questions; If there is a posibility, and of interest to find out: What could have been done better on the different systems? Is there any optimal systems? And what about a standard system? Is there any possibility for a low-fi prototype that illustrates weakness and strength of a system?

Otherwise we wish the group good luck in the future work. J