



## MSc Project Plan

### Security assessment of authentication technology in a hostile environment

Roar S. Sollie  
roar.sollie@hig.no  
Mobile phone: 48223904

NISlab  
Gjøvik University College

December 17, 2004

## Revision History

Version #	Changes implemented; motivation, nature and location
0.1	This is the first version of the project plan.
0.11	Edited the topic and added a research question.
0.21	Added Review of State of the Art.
0.22	Modified topic, and problem description.
0.23	Added more to Review of State of the Art.
0.31	Added Summary of Claimed Contributions.
0.32	Added information in section 1.3. Stakeholders and motivation.
0.33	Changed research question in section 2.3 to compareness.
0.41	Added Choice of Methods.
0.42	Changed one research question and removed one.
0.43	Added a research question regarding user-friendliness.
0.44	Trying to define an experiment in Choice of Methods-chapter.
0.51	Adding Milestones, deliverables and resources, Feasibility Study, Risk Analysis, and Ethical and Legal Considerations.
0.52	Changed topic, making adjustments according to the feedback from the supervisor.
0.6	Making the final adjustments like spelling, grammar and rephrasing.
1.0	MSc Project Plan

## **Abstract**

In today's modern society, one has certain requirements to the technology. You want to be able to access and perform tasks regardless of time and location. The problem that occurs is how one can be sure that a person is the one he or she is claiming to be. How can one have a secure validation of identity in an insecure environment? Is it possible to have such implemented security routines that one can be sure of a person's identity? Personnel can be authenticated using something the person is, has or knows.

The purpose of this project is to see if it is possible to combine different authentication methods, both biometrical and technical, and how this will affect the security of the overall authentication routine. How much is security improved when the authentication procedure includes a combination of something one is, knows or has, e.g. a procedure including both a password and a smart card? How will this affect the usability? One may also use two or more approaches from the same category, e.g. using face recognition and fingerprint which both are in the category referred to as something one is. Will it make the authentication system stronger or weaker?

# Contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
1.1	Topic Covered by This Thesis . . . . .	5
1.2	Problem Description . . . . .	5
1.3	Justification, Motivation and Benefits . . . . .	5
1.4	Research Questions . . . . .	6
<b>2</b>	<b>Review of State of The Art Related to the Resarch Questions</b>	<b>7</b>
2.1	Review of different authentication methods. How Secure is an Authentication Method in a Secure Environment vs. an Insecure and Uncontrolled Environment? . . . . .	7
2.2	Comparison of Various Authentication Methods. How Will Security be Affected by Combining Two or More Authentication Methods? . . . . .	7
2.3	To which extent will the security affect the level of user-friendliness? How will a combination of authentication methods affect this issue? . . . . .	9
2.4	Is the Implementation of Two or More Authentication Worth the Effort(Cost/Benefit)? . . . . .	9
<b>3</b>	<b>Summary of Claimed Contributions</b>	<b>9</b>
<b>4</b>	<b>Choice of Methods</b>	<b>10</b>
4.1	Review of different authentication methods. How Secure is an Authentication Method in a Secure Environment vs. an Insecure and Uncontrolled Environment? . . . . .	11
4.2	Comparison of Various Authentication Methods. How Will Security be Affected by Combining Two or More Authentication Methods? . . . . .	11
4.3	To which extent will the security affect the level of user-friendliness? How will a combination of authentication methods affect this issue? . . . . .	11
4.4	Is the Implementation of Two or More Authentication Worth the Effort(Cost/Benefit)? . . . . .	11
<b>5</b>	<b>Milestones, Deliverables and Resources</b>	<b>12</b>
5.1	Schedule . . . . .	12
5.2	Resources . . . . .	14
5.3	Preliminary table of contents for the MSc thesis . . . . .	15
<b>6</b>	<b>Feasibility Study</b>	<b>15</b>

<b>7 Risk Analysis</b>	<b>16</b>
<b>8 Ethical and Legal Considerations</b>	<b>16</b>

# **1 Introduction**

## **1.1 Topic Covered by This Thesis**

Methods for security assessment of authentication technology in a hostile environment (strength of function).

## **1.2 Problem Description**

Known and traditional authentication methods, for example traditional passwords, PIN-code or question-and-answer, suffer sometimes from known and exploitable weaknesses. A password is something one ought to remember, and is often based on words, which can be guessed easily. PIN-codes are seldom longer than four digits, which makes them easy for an adversary to find if there is no mechanism to control the number of attempts. Stronger authentication methods, e.g. smart cards, fingerprints, iris patterns and face recognition, also suffer from some known weaknesses. This is mostly because the authentication takes place in an insecure environment.

How will it affect security if one combines two or more authentication methods? Which combinations will lead to the strongest security of the overall authentication system? How will this affect the issue of security vs usability? What influence on the cost/benefit analysis will an implementation of such system have?

## **1.3 Justification, Motivation and Benefits**

Verification of the identity of a person is important having in mind the possibility of theft and fraud of both money and identity. If security is compromised, privacy is likely to be compromised as well. The whole information environment is based on trust. Stakeholders for such knowledge and information would be anyone in need of strong authentication methods and other people interested in authentication.

Implementation of strong authentication methods is important in the strategy of securing information, especially in organisations where it is critical for the information security that no unauthorized entities gain access to these information systems. In systems with information regarding money transactions and sensitive personal information, it is critical to have strong authentication methods in order to be protected against fraud and unauthorized use or leakage of information. The dilemma however is whether the level of security will affect the overall usability of the system.

## 1.4 Research Questions

- How Secure is an Authentication Method in a Secure Environment vs. an Insecure and Uncontrolled Environment?
- How Will Security be Affected by Combining Two or More Authentication Methods?
- To which extent will the security affect level of user-friendliness? How will a combination of authentication methods affect this issue?
- Is the Implementation of Two or More Authentication Worth the Effort(Cost/Benefit)?

## **2 Review of State of The Art Related to the Research Questions**

### **2.1 Review of different authentication methods. How Secure is an Authentication Method in a Secure Environment vs. an Insecure and Uncontrolled Environment?**

In [1], the problems of measuring information security and identifying good authentication practises have been discussed.

In [2], the problems of authentication have also been discussed, and the uncertainty inherent to authentication decisions has been emphasised.

In 1994 NIST published FIPS 190 [3], a guideline describing the primary alternative methods for verifying the identities of computer system users. It states that single password authentication systems are too weak, and that one should use passwords, tokens, and biometrics in different combinations to achieve better assurance in the authentication system.

[4] explores the complications when attempting to create a secure pervasive computing environment. It discusses challenges in both physical and information security, and the fact that authorisation, auditing and non-repudiation all rely on an accurate identification and verification of the user.

In [5] threats to smart cards are described and a security model of a smart cards system is discussed independently of its application. A trust environment is modelled and all potential parties involved in any smart card system: the cardholder, the terminal, the data owner, the card issuer, the card manufacturer, and the software manufacturer.

In [6] many important issues, also related to the other research questions, are discussed. These include for example: ease of use, applicability, speed of verification, vulnerability to fraud, size of storage and multiple authentication technologies. This book shows the basic concept of biometrics and explores biometric technologies to various applications in an e-world (electronic world).

### **2.2 Comparison of Various Authentication Methods. How Will Security be Affected by Combining Two or More Authentication Methods?**

In [7] it is discussed how the combination of smart card and biometric authentication, e.g. fingerprint, will affect security. [7] also compares the level

of security achieved in such a system with the traditional PIN authentication system.

[8] describes how combining several biometric authentication methods improves the accuracy and decreases false-positives and false-negatives, to the level which cannot be achieved with a single-model biometric solution.

[9] discusses and compares usability between the password authentication method and other authentication methods, for example pass faces. It also takes into consideration that token-based biometric, and other authentication methods, often require special and expensive hardware.

In [10], the integration of two biometric techniques, voice and face recognition, as well as the potential benefit of combining these techniques in order to improve the robustness of person identification. It is mentioned that the combination of these techniques is capable of identifying persons with high accuracy under tightly constrained conditions. In addition to face and speech recognition, [11] combines these with observing lip motions. The results of this experiment show that the integration of two or three techniques, leads to better recognition rates.

[12] refers to how secure smart cards are, their potential vulnerabilities, their security and presents a cost/benefit analysis of their application. The paper [12] will therefore be an important reference in further work regarding smart cards in this thesis.

In [13], several authentication methods are described, as well as advantages and disadvantages of those methods. The paper, [13], can therefore be referred to as a well-describing basic paper for people interested in authentication research.

Various authentication methods are described in many more articles and papers. For example [14] considers hash visualization in user authentication, and a prototype where a user authenticates by recognizing a set of previously seen images has been described. In [15], the same problem as in [14] is analyzed in more detail.

[16] describes various authentication methods: password, token and biometric authentication. It compares different authenticators by weaknesses and strengths, states that human authentication is a critical concern for corporate security and provides insight into advantages and disadvantages of current options.

In [17], the authors try to describe what makes a biometric system more secure than another one as well as the differences among various systems. Parameters mentioned are: liveness testing, tamper resistance, secure communication, security threshold level and fall-back mode.

[18] and [19] provide an excellent overview of personal authentication mechanisms.

### **2.3 To which extent will the security affect the level of user-friendliness? How will a combination of authentication methods affect this issue?**

[20] describes different aspects of authentication, the issue of authentication and privacy, and the issue of security and usability. One of the crucial factors that will encourage or discourage the use of any authentication technology is ease of deployment. A scheme that relies on something that users already have (or already "are") is easier to deploy than one that requires shipping (and perhaps installing) of new equipment.

In [21] the issues of usability, acceptability and privacy in the biometric authentication environment are discussed. The sensors are getting smaller, cheaper, more reliable, and designed with better ergonomic characteristics. The biometric algorithms are also getting better, and many systems include features to train the users and provide feedback during the exploitation. Hopefully this will help to make biometric authentication more usable and acceptable.

[17] describes usability of biometric authentication methods and discusses central issues regarding failure to enrol(FTE), false acceptance rate(FAR) and false rejection rates(FRR).

### **2.4 Is the Implementation of Two or More Authentication Worth the Effort(Cost/Benefit)?**

There are several articles, e.g. [9] and [12], bringing up the cost/benefit-question when they evaluate different authentication methods.[12] concludes that organisations, implicitly or explicitly, make decisions based on whether the cost of the decisions is justified by the benefit, and that these determinations often are more subjective than objective. If the cost of the new feature is less than the value of the reduced risk plus any additional benefits provided by the card, then the device should be implemented.

## **3 Summary of Claimed Contributions**

Existing literature provides information about different authentication techniques and how they are used, but none of these provide information about authentication methods in a secure environment vs. an insecure environment. Little is written about how different combination of authentication methods affect the level of security and cost/benefit analysis of these solutions is seldom given.

This thesis will therefore try to provide some answers to the research questions which are not covered in the literature. A collection of experiences from Norwegian companies and organizations regarding the use, development and exploitation of different authentication methods will be presented.

An experiment will also be conducted that hopefully will contribute to the evaluation of various authentication methods, from the aspect of complexity, level of security and usability.

## 4 Choice of Methods

A qualitative method seems to be appropriate for answering my research questions. In [22] it is described that a qualitative method intends to create a deeper understanding of the problem complexity. [23] provides additional information to the choice of method and describes the work from formulating questions to seeking and finding solutions.

A literature study will be performed to gain information and knowledge about the various authentication methods and the environment in which they are implemented. The purpose of this literature study is to be able to make some conclusions about the strength of different methods, and to be able to see which combinations are best suited to the use in an insecure environment.

An experiment will be conducted mainly in order to try to measure the time of execution using different authentication methods with different algorithms to see if a trade-off between the execution time and the security is achieved. It is important to normalize these times, making it possible to compare the security. The question is how much the security will be impaired by this normalization. Hopefully this experiment will contribute to an estimation of acceptable delay (waiting time/response time), and compare the level of security when different methods of authentication are normalized. The experiment will be focused on the use of smart cards and passwords, using different cryptographic algorithms, lengths of keys and necessary numbers of operations. One of the important issues is the time of execution, and to which extent this will affect the usability and user-friendliness of different algorithms and methods of authentication. This experiment will hopefully help answering the research questions and act as a basis for the conclusions.

#### **4.1 Review of different authentication methods. How Secure is an Authentication Method in a Secure Environment vs. an Insecure and Uncontrolled Environment?**

A literature study will hopefully give an answer to how different methods of authentication work in different environment and how the environment may affect the level of security.

#### **4.2 Comparison of Various Authentication Methods. How Will Security be Affected by Combining Two or More Authentication Methods?**

Theoretical analysis based on a literature study should give an answer to this research question. The use of scientific search engines, workshops and conferences, will be valuable and relevant for this work. Research and analysis of other experiments, studies and tests will also provide valuable information. The evaluation of different authentication methods will be based on this information.

#### **4.3 To which extent will the security affect the level of user-friendliness? How will a combination of authentication methods affect this issue?**

Literature study based on related tests and experiments will be used to answer these questions. Hopefully a small experiment will be carried out with an authentication method and a combination of methods.

#### **4.4 Is the Implementation of Two or More Authentication Worth the Effort(Cost/Benefit)?**

Basically the same procedure as with the research question above in addition to an analysis of the cost in buying and installing the different methods, will be performed.

The experiment will hopefully give an answer to the questions regarding combinations of algorithms, key lengths, complexity and encryption and that will contribute to the solution of the questions related to cost and benefit. Time of execution and level of security is an essential topic to help evaluate

this question. This experiment will also contribute to the evaluation of user-friendliness and compareness of different authentication methods.

## 5 Milestones, Deliverables and Resources

Resources needed to perform the project, besides contact person, will be different authentication equipment connected and integrated to a computer system. I do not have a complete list of equipment needed, but it will include e.g. smart cards, smart card readers, application needed to test the authentication(e.g. login) etc.

Table 1 shows an overview for the main activities and estimated time used to perform these activities. Preparing the experiment includes installation, implementation and get the equipment needed to perform the experiment.

No information has been given as to deliverables during the conduction of MSc thesis at this moment. I believe it is reasonable to present the work done so far, once a month. This will make it possible for the teaching supervisor and contact persons at Buypass.as to come up with suggestions and directions for further work.

### 5.1 Schedule

The project is defined in an early stage, the estimation of time needed may vary in both ways. In order to schedule the workload I have tried to put together an overview of estimated time needed in Table 1 and a more detailed description of estimated hours needed to conduct the various activities in Table 2.

<b>Activity</b>	<b>Hours needed</b>	<b>Start time</b>	<b>End time</b>	<b>Contributors and resources</b>
Literature study	130	W2	W10	Library at HiG, scientific search engines, workshops and conferences
Preparing experiment(research, installation, and implementation)	110	W4	W10	Teaching supervisor, contact persons at Buypass.as and NISlab
Conducting the experiment	90	W11	W14	Equipment at NISlab and contact persons
Discussion and evaluation of experiments and results, and trying to answer the research questions.	90	W17	W19	Results from the experiment, contact person and teaching supervisor
Conclusion. What is done and are the results/conclusions achieved.	50	W23	W24	Results from the experiment.
Prepare presentation	40	W21	W22	MSc thesis and teaching supervisor
Write thesis report(all versions)	200	W2	W26	Teaching supervisor, contact persons at Buypass.as and HiG
Total	710	W2	W26	

Table 1: Overview: Activities, Deliverables, Resources and Milestones

Week	Hours	Activities
2	30	Literature study(30)
3	25	Literature study(20), write thesis report(5)
4	30	Literature study(20), prepare experiment(10)
5	25	Literature study(10), prepare experiment(15)
6	30	Literature study(10), prepare experiment(10), write thesis report(10)
7	25	Literature study(10), prepare experiment(15)
8	25	Literature study(10), prepare experiment(15)
9	30	Literature study(10), prepare experiment(10), write thesis report(10)
10	30	Literature study(10), prepare experiment(20)
11	25	Prepare experiment(10), conduct the experiment(15)
12	20	Easter, conduct the experiment(20)
13	30	Conduct the experiment(30)
14	30	Conduct the experiment(30)
15	30	Write thesis report(30)
16	25	Write thesis report(25)
17	30	Discussion(30)
18	30	Discussion(30)
19	30	Discussion(30)
20	25	Exam, conclusion(25)
21	35	Write thesis report(15), prepare presentation(20)
22	30	Prepare presentation(20), write thesis report(10)
23	35	Conclusion(25), write thesis report(10)
24	30	Write thesis report(30)
25	35	Write thesis report(35)
26	20	Write thesis report(20)
Total	710	

Table 2: Detailed: Activities, Deliverables, Resources and Milestones

## 5.2 Resources

Resources needed to perform the experiment will be smart cards, smart card readers, applications which makes it possible to change length of keys and cryptographic algorithms.

## 5.3 Preliminary table of contents for the MSc thesis

1. Introduction
  - 1.1. Topic covered by the thesis
  - 1.2. Problem description
  - 1.3. Justification, motivation and benefits
  - 1.4. Research questions
2. Background - Review of state of the art
  - 2.1 Subsections for each research question
3. Choice of methods
  - 3.1. Sub sections for each research question
  - 3.2. Definition of quantitative metrics for evaluation of security and usability
4. Project results
  - 4.1 Results of the experiment
  - 4.2 Further work
5. References
6. Appendix

## 6 Feasibility Study

Based on the estimated workload of 710 hours, distributed over 25 weeks(2-26), combined with part time work, I believe it is feasible. If I need more time it is possible to use evenings and weekends as well.

The accomplishment of the literature study and selection of different methods of authentication for the experiment will be essential and important for the remaining parts of the thesis.

The installation and testing of various algorithms and methods of authentication will be a critical task. NISlab, Buypass.as and the staff at Gjøvik University College will hopefully contribute to make this feasible.

## 7 Risk Analysis

I believe the project is feasible within the time limits and resources available. One problem however, will be how to narrow the project into specific solutions and methods of authentication, to be able to carry through the experiment and come up with interesting results or conclusions. If I somehow fail to conduct some of the tasks or research methods, I believe the failure itself will bring some interesting results and answers. Table 3 describes possible risks and tries to make suggestions about how to solve them and possible consequences.

## 8 Ethical and Legal Considerations

Special care will be taken in order to ensure that "business confidential" information is not revealed. Vendors and contributors will be informed about the experiment and the fact that results and conclusions will be published in the final MSc thesis report. Vulnerabilities and strengths of various solutions tested and evaluated will be addressed, and if this information has not already been made public, special care will and must be taken. In such cases information must be revealed and permissions must be obtained.

<b>Problem</b>	<b>Consequences</b>	<b>Solution</b>
Difficulties conducting the experiment.	Some difficulties will themselves give some answers important for the results. If the difficulties are caused by lack of knowledge and experience it is not for sure that the experiment will contribute any results or conclusions.	Obtain more resources and/or personnel willing to help conduct the experiment.
The contact persons is not able to help conducting the experiment.	This will hopefully only cause a minor delay, but may cause the deadline to be postponed.	Find other persons willing to help contribute.
Unable to get hold of equipment for the experiment.	The experiment is not feasible, or the experiment will have to be conducted in a lower scale.	Try to get hold of other equipment in other places, by other vendors or developers.
Diminishing health of the author or close family.	Short time sickness will delay the project. Long-term sickness will cause the deadline of the project to be moved or postponed.	Impossible to prevent oneself against such causes, and this threat will always be there. Help from contributors and contact persons will help complete the thesis in the case of short time sickness.

Table 3: Risk analyses: Possible problems, consequences and solutions

## References

- [1] Applied Computer Security Associates. Workshop on information security system scoring and ranking, 2001. <http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf>.
- [2] G. R. Ganger. Authentication confidences. <http://citeseer.ist.psu.edu/456656.html>, 2001. Technical Report CMU-CS-01-123.
- [3] NIST. Fips 190, guideline for the use of advanced authentication technology alternatives, 1994. <http://www.itl.nist.gov/fipspubs/fip190.htm>.
- [4] Patrick G. McLean. A secure pervasive environment. In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*, pages 67–75. Australian Computer Society, Inc., 2003.
- [5] Bruce Schneier and Adam Shostack. Breaking up is hard to do: Modeling security threats for smart cards, 1999. [http://www.usenix.org/publications/library/proceedings/smartcard99/full%\\\_papers/schneier/schneier\\\_html](http://www.usenix.org/publications/library/proceedings/smartcard99/full%\_papers/schneier/schneier\_html).
- [6] David D. Zhang, editor. *Biometric Solutions For Authentication in an E-World*. The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, 2002.
- [7] L. Bechelli, S. Bistarelli, and A. Vaccarelli. Biometrics authentication with smartcard, 2002. <http://citeseer.ist.psu.edu/bechelli02biometrics.html>.
- [8] N. Poh, S. Bengio, and J. Korczak. A multi-sample multi-source model for biometric authentication, 2002. <http://citeseer.ist.psu.edu/thian02multisample.html>.
- [9] S. Brostoff and A. Sasse. Are passfaces more usable than passwords? A field trial investigation., 2000. [http://oneman.cs.ucl.ac.uk/brostoff\\\_sasse.pdf](http://oneman.cs.ucl.ac.uk/brostoff\_sasse.pdf).
- [10] Timothy J. Hazen, Eugene Weinstein, and Alex Park. Towards robust person recognition on handheld devices using face and speaker identification technologies. In *Proceedings of the 5th international conference on Multimodal interfaces*, pages 289–292. ACM Press, 2003. <http://doi.acm.org/10.1145/958432.958485>.

- [11] Niall A. Fox, Ralph Gross, Philip de Chazal, Jeffery F. Cohn, and Richard B. Reilly. Person identification using automatic integration of speech, lip, and face experts. In *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, pages 25–32. ACM Press, 2003.
- [12] John Abbott. Smart cards: How secure are they? *GSEC Practical v1.3*, 2002. <http://www.sans.org/rr/papers/index.php?id=131>.
- [13] Marilyn Chun. Authentication mechanisms, which is best?, 1995. [http://www.giac.org/practical/gsec/Marilyn\\_Chun\\_GSEC.pdf](http://www.giac.org/practical/gsec/Marilyn_Chun_GSEC.pdf).
- [14] R. Dhamija. Hash visualization in user authentication, 2000. <http://citeseer.ist.psu.edu/dhamija00hash.html>.
- [15] Rachna Dhamija and Adrian Perrig. Dejà vu: A user study using images for authentication. In *Proceedings of the 9th USENIX Security Symposium*, 2000. <http://citeseer.ist.psu.edu/326534.html>.
- [16] Lawrence O’Gorman. Securing business’s front doors - password, token, and biometric authentication, 2002. <http://www.research.avayalabs.com/techreport/ALR-2002-042-paper.pdf>.
- [17] Vaclav Matyas and Zdenek Riha. Biometric authentication-security and usability. [http://www.fi.muni.cz/usr/matyas/cms\\_matyas\\_riha\\_biometrics.pdf](http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf), 2002. Faculty of Informatics, Masaryk university Brno, Czech Republic.
- [18] Chiara Braghi. Biometric authentication. <http://citeseer.ist.psu.edu/436492.html>.
- [19] Richard E. Smith. *Authentication: From Passwords to Public Keys*. Addison-Wesley Pub Co, 2001.
- [20] Stephen T. Kent and Lynette I. Millett. *Who Goes There?: Authentication Through the Lens of Privacy*. CSTB Publications, 2003.
- [21] Andrew S. Patrick. Usability and acceptability of biometric security systems. *Lecture Notes in Computer Science*, 3110 / 2004, 2004.
- [22] John W. Creswell. *Research Design; Qualitative, Quantitative and Mixed Methods Approaches*. Sage Publications, second edition edition, 2003.
- [23] Neil J. Salkind. *Exploring Research*. Prentice Hall, 5th edition, 2002.

## Appendix

#	Date	Version	Problem	Remedy	Status
1	29.10.2004	0.31	Who are the stakeholders? Section 1.3 is thin.	Added information	OK
2	29.10.2004	0.31	Change of research question in section 2.3.	Changed question	OK
3	29.10.2004	0.31	Paper about authentication methods in Esorics 2004	Received paper	OK
4	31.10.2004	0.41	Insecure in deciding the choice of methods.	Talked to Slobodan Petrovic	OK
5	08.11.2004	0.41	More and specific information on "Choice of Method"	Talked to Slobodan Petrovic	OK
6	08.11.2004	0.43	Rephrasing and modifying "Claimed Contributions.	Talked with teaching supervisor, Slobodan Petrovic	OK
7	12.12.2004	0.51	Change topic, it is too wide. More information in "Choice of Method"	Teaching supervisor and lecturers	OK
8	15.12.2004	0.52	Add information to "Choice of Method": normalize execution times in order to be able to compare security and usability.	Teaching supervisor	OK
9	16.12.2004	0.52	Need more "Peer Reviewed"-articles	Talked to supervisor, said it was enough	OK
10	17.12.2004	0.6	Making the final adjustments like spelling, grammar and rephrasing.	teaching supervisor	OK