Security for Databases stored on Smart Cards; Query Processing, Data Access and Data Storage.

1 Statement of Objectives.

1.1 What do I intend to achieve?

- Investigate existing proposals of how a database would be stored on a smart/card token and find more areas where this could be used, apart from the examples already found in published papers [3].
- Review current standards which are related to databases or SQL and also investigate alternative ways in which data is being stored and recorded on a smart card such as:
  - using SQL queries instead of HTTP requests and web services to get the data needed from a database.
  - storing a database instead of a transparent (binary) file.
- Provide suggestions and recommendations for the development and operation of a secure system to process transactions, store the database and find a suitable location of where it should be stored.
- Consider aspects such as:
  - Access Control
  - Selective Data Dissemination
  - Difference between data privacy and confidentiality when querying data from a database which requires the user's consent. In a centralised server database this is still a problem because an intruder might log as a database administrator and get the data in clear text.
  - Execution of efficient queries over encrypted data.
- Review from a security point of view the security for each of the stages in accessing and querying a database i.e.

- Cryptography for query processing
- Protection against data: snooping, altering, substituting and replaying.
- Identify techniques on how to keep the integrity of the protected data units (PDUs) [1] which would be defined in a database.

1.2 Why have I chosen the proposed project?

I am proposing the above project title because during the past 5 years I spent in industry, I worked for an Information Systems development company as a software developer specialising in MS SQL, and one of my main areas of expertise is databases and SQL.

So while I was thinking what area should I focus on, I started to focus my search on SQL and Smart Cards. This led to a vast and rich volume of information on smart cards and a lacuna on the uses of databases in the smart card environment. This fact challenged me to research more about the subject and I started to notice that throughout the years, the industry, with the help of scholars and researchers in the area already tried to do something [2], [4], [1], [5] but till now no real applicability of this technology has emerged. In my opinion this could be because at present not much data can be stored on a smart card (capacity constraints), this though will change with the introduction of higher memory chips and SSMSC devices (Smart Secured Mass Storage Cards).

I hope that with my knowledge and expertise in the database area, accompanied by more research, I will be able to contribute and come up with some interesting proposals and hopefully, discoveries or novel ideas.

2 Methods to be used.

2.1 How do I intend to achieve the objectives listed above?

I will tackle the objectives by:

1. Researching the subject and find out about current studies which are available.
2. Where possible contact people and companies who already did research and development in this area to learn about the latest developments.
3. If simulators exist, to simulate high capacity storage and simulation of database queries (SQL?) on an on board database, these will be tried out.
4. Compile a list of threats and attacks and attempt to find countermeasures for each.

5. Study the ISO/IEC 7816-7 standard and question/investigate why it hasn't yet captured a market interest, maybe also come up with enhancements and criticism to this section of the standard.

6. Ask the following questions:

   - Why Database on a Smart Card instead of a Centralised Protected Database on a Server?

     My proposal is suitable for databases where:
     - The data must be highly available (anywhere, anytime, on any terminal and without requiring a network connection).
     - The storage of sensitive data on a centralised server might put data privacy at risk.
     - Maintenance of one centralised database is very complex due to the variety of data sources from where the data is coming.

     Whilst having all these advantages we must not forget that there might also be disadvantages on having a database on a smart card such as:
     - What happens if the card is lost or destroyed?
     - Is there need to still keep a backup somewhere on an archive database?
   - What kind of Smart Card can be used?

     SUMO Card by GEMPLUS? (if it still exists) or any other smart card/token with higher memory.
   - What kind of attacks can happen on an implementation like this?
     - Data/Query Snooping
     - Data/Query Altering
     - Data/Query Substituting
     - Data/Query Replaying
     - Maybe others?

2.2 What is your strategy for getting started

Having a good strategy to start with is very important as it will pave the way ahead to build up my project.

- Start reading all relevant information that can be found in books, Internet, papers, reports, companies and other students and researchers who have worked on this idea before.
- Literature Review
- Develop chapters for each of the points listed in the objectives above.

- Come up with proposals (if possible) on each and every objective.
- In my conclusions I will state what the objectives of this project were and whether they have been achieved also giving reasons if any objective was not met.

3 The Work Plan

Keeping in mind that during the second semester for my *M.Sc.* degree I need to attend to lectures, study the new subject I have this semester, revise subjects from semester one and prepare for the exams in May; the following weeks will be weeks focused more on expanding my knowledge on the subject and prepare information so that once exams are over I will start working harder on the objectives listed in the first section.

3.1 Schedule

	Feb	Mar	Apr	May	Jun	Jul	Aug
Data Collection	✓	✓	✓	✓			
Data Analysis		✓	✓	✓	✓		
Data Comparison					✓	✓	
Literature Review	✓	✓	✓	✓	✓	✓	✓
Progress Review Against Project Schedule	✓	✓	✓	✓	✓	✓	✓
Correspondence with Supervisor	✓	✓	✓	✓	✓	✓	✓
Conclusions						✓	✓

Table 1: M.Sc. Project Schedule 2010

3.2 Draft *Table of Contents*

Please note this is a draft table of contents and that it may vary from the one that will be delivered at the end of the Project.

1. Introduction
   (a) Project Background
   (b) Project Aim
   (c) Project Objectives
   (d) Project Approach
2. Smart Cards/Tokens
   (a) Hardware

(b) Software
(c) Operating Systems
(d) Memory and Storage Capacity
(e) Speed and Efficiency

3. Databases
   (a) Database Models
   (b) Query Languages - DDL and DML
   (c) Smart Card Standard for databases
4. Security related to Smart Cards and Databases.
5. Why Smart Cards and Databases?
6. A Case Study Model
7. Simulating a Database on a Smart Card/Token
8. How to handle the Security issues of such a device?
   (a) Access Control
   (b) Data Privacy vs Data Confidentiality
   (c) Cryptography for Query Processing
   (d) Execution of encrypted queries over encrypted data
   (e) Attacks on Data: Snooping, Altering, Substituting and Replaying
   (f) Any Countermeasures (introduce notion of data degradation)
9. Remarks and Conclusion

4 Additional Comments

No additional comments.

References

[1] Nicolas Anciaux. *Systèmes de gestion de base de données embarqués dans une puce électronique(Database Systems on Chip).* PhD thesis, Université de Versailles-Saint Quentin en Yvelines, 12 2004.

[2] Nicolas Anciaux, Mehdi Benzine, Luc Bouganim, Philippe Pucheral, and Dennis Shasha. Ghostdb: querying visible and hidden data without leaks. In *SIGMOD '07: Proceedings of the 2007 ACM SIGMOD international conference on Management of data*, pages 677–688, New York, NY, USA, 2007. ACM.

[3] Nicolas Anciaux, Morgane Berthelot, Laurent Braconnier, Luc Bouganim, Martine De la Blache, Georges Gardarin, Philippe Kesmarszky, Sophie Lartigue, Jean-François Navarre, Philippe Pucheral, Jean-Jacques Vandewalle, and Karine Zeitouni. A tamper-resistant and portable healthcare folder. *Int. J. Telemedicine Appl.*, 2008:1–9, 2008.

[4] Nicolas Anciaux, Luc Bouganim, Philippe Pucheral, and Patrick Valduriez. Disc: Benchmarking secure chip dbms. *IEEE Transactions on Knowledge and Data Engineering*, 20:1363–1377, 2008.

[5] P. PUCHERAL. Picodbms : Scaling down database techniques for the smartcard. *The VLDB Journal*, 10(1):120–132, 2001.

To be completedby Project Supervisor

I approve the attached project plan.

Signature (Supervisor)	Signature (Student)
Date:	Date: