CS499 End Semester Report

Smart Card based application for IITK Swimming Pool management

Submitted By: Ankur Mittal
Project Guide: Prof. Rajat Moona

Certificate

This is to certify that the work contained in this report entitled "Smart Card based application for IITK Swimming Pool management", by Ankur Mittal (Y2077), has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

May, 2007.

(Dr. Rajat Moona)
Department of Computer Science and Engineering,
Indian Institute of Technology, Kanpur.

Introduction

In today’s world, there is an increasing need for digitized information. People prefer to show their identity card and avail a service rather than to prove their identity on paper. We must make sure that the exchange of information is secure and as efficient as the conventional methods.

1.0 Problem Statement

Nowadays, anyone who is a member of the swimming pool and wants to access it has to sign in the necessary information into the given register. We plan to digitize this method and use their smart cards as means of authorization.

In the swimming pool project, we aim to use IITK smart ID as the IITK swimming pool card using which the Swimming pool user can mark his entry and exit.

1.1 Entities in the System

The following entities constitute our swimming pool application:

1. **Application Creator Authority (ACA) –** The ACA card is issued by the ID cell to the Swimming Pool Registration Authority (SPRA). The SPRA needs ACA card in order to create a new Swimming Pool Application on the IITK smart ID. In this card, a Swimming Pool Master Key is stored separately. The ACA card with Swimming Pool Master Key is known as SPRA card in this document.

2. **Swimming Pool Registration Authority (SPRA**) – The SPRA registers the user as a Swimming pool member i.e. it enables the Swimming Pool Application. The user can choose if he wants to have a fixed number of swims i.e. limited swims or he wants to use the pool regularly for a fixed number of months i.e. regular user. The user has to pay the required fees to the SPRA to get registered.

3. **Front Desk Operation –** When the Swimming pool member wants to enter the swimming pool, he enters his IITK smart card enabled with Swimming Pool Application in one of the readers available at the front desk. This will mark the entry of the user in the Swimming pool and his name will appear in the list of the members inside the pool. While exiting, the member again inserts his card in the reader which will mark his exit and he can see his name in the exit card.

1.2 Registration Process

To register as a Swimming Pool user, a person has to get an IITK smart Card issued to him. This is done by the ID cell. Then, the person has to go to the Swimming Pool Registration authority. The SPRA can register the person as a swimming pool user, using the SPRA Card. If the person was already registered in the Swimming Pool in the past, the SPRA will find the corresponding entry in the Swimming Pool Registration Database as well as on the IITK smart ID. In this case, SPRA will just update the registration database and information regarding the user in the IITK smart ID.

In addition to registration, SPRA will also receive the daily logs from the Front Desk, update the Daily log database and search it for entry/exit log of some member.

1.3 Front Desk Operations

When a Swimming Pool member is entering the swimming pool, the Front Desk Attendant will supervise the entry/exit of Swimming Pool members. The attendant will oversee the entry/exit of the on the display. In case a member who is not from the current slot wants to enter the pool, the attendant can allow/deny him permission depending on the strength of the members inside the Swimming Pool.

The attendant can also see the entry/exit list of any slot and can manually mark the exit of members who did not mark their exit.

The attendant will also transfer the daily logs to a storage device (USB mass storage device or a floppy) connected to the Front Desk Computer. This can be taken to the SPRA for consolidation. Also, the attendant can manually change the
Configuration file of Slots in case slot timing has been changed.

1.4 Cards Involved in the Process

1.4.1 **ACA Card –** This card issued by the ID cell to the SPRA is used to register all the new members of the Swimming Pool i.e. the members who have never used the pool in the past. For later updates to the member cards, only the Swimming Pool Master Key will be needed. The Swimming Pool Master Key will be kept in the ACA card itself and it will be called SPRA card. Thus a single SPRA card is used to create new members or to update existing members.

1.4.2 **Front Desk Card –** This card is issued by the SPRA to the Front Desk Attendant. This card is inserted in one of the smart card readers available at the Front Desk in case the Swimming Pool member data needs to be updated and also to authenticate whether the user is a valid swimming pool user or not.

1.4.3 **Member Card –** This is the IITK smart ID with the Swimming Pool Application on it. In this card, all the data regarding the Swimming Pool member (i.e. limited swim user/regular user, slot number, validity, and date of registration) is stored.

1.5 Key Management

There are 3 keys involved in the process:

1.5.1 ACA key – This key is written by the ID cell in the ACA card. This key is used for authenticating the User Card with the ACA Card in order to create an application on the card. Using this key, the files related to the Swimming Pool Application are created.

1.5.2 Swimming Pool Master Key – This key is decided upon by the SPRA and is written on the ACA card and the Front Desk Card. This key is used by the SPRA to update data in the files of the Swimming Pool Application in the user card. This key is also used at the Front Desk in order to externally authenticate the IITK smart ID with the Front Desk card to decrease the swim counts of Limited Swim members.

1.5.3 Per Card Swimming Pool Key – This key is derived from the Swimming Pool Master Key using the ID (PF No. /Roll No.) of the member. This key which is stored in the member card is used for authentication of the member at the Front Desk and also by the SPRA in order to update the Swimming Pool User's data.

1.6 Data Structure on Cards

1.6.1 IITK smart ID – On the IITK smart ID, the Swimming Pool Application has been allotted the DF (Dedicated File) 6F00 under the MF (Master File). Under the DF, EF02 stores the Per Card Swimming Pool Key required for authentication in case the Swimming Pool User's data needs to be updated. This key is generated by encrypting the User ID (data) using the Swimming Pool Master Key as the key. Hence, the data can only be modified using the SPRA Card or the Front Desk Card.
Under the same DF, the information related to the swimming pool user (i.e. limited swim user/regular user, slot number, validity, and date of registration) is stored in the EF03 file under the same DF (refer to the File Structure for more information). The usage of update command in this EF is protected and it can be executed only on authentication with the Swimming Pool Master Key

1.6.2 Front Desk Card – This card stores the Swimming Pool Master Key in the Elementary File EF02 under the Dedicated File 7F00. The Swimming Pool Master Key is stored in the EF 7F02 (no read permission) can only be used in its derived form (to get the Per User Swimming Pool Key) and can be used for internal and external authentication in order to validate itself and the

FD/SPRA card. These conditions have been set in the Elementary File 7F03 in Security Environment # 1.

1.6.3 **ACA Card –** This card stores the ACA Key provided by the ID Cell. The Swimming Pool Master Key is stored in the Elementary file 7F02 and is stored as a data item. The data is password protected. These security conditions have been set in the Elementary File 7F03 in Security Environment # 2.

1.7 Card Involvement in the process

The IITK smart Card will be used in digitizing the Swimming Pool Registration and the Front Desk Operations.

1.7.1 **Registration Process –** During the registration time, the SPRA will create the DF (Dedicated File) 6F00 (DF allocated to the Swimming Pool Application) and the EFs (Elementary File) under this DF corresponding to the Swimming Pool Application in the IITK smart Card using the Swimming Pool Master Key. If the user was registered in the past, these files would be existent and the SPRA will update the information relating to the user in the EF03 file.

1.7.2 **Front Desk Operation –** While entering the Swimming Pool, the application reads the Swimming Pool User Information from the smart Card, and checks if he is registered in the current slot or his number of swims has not expired. Then, it permits the user to enter the Swimming Pool. In case of Limited Swims user, the Application will also decrement the number of swims of the member using the Swimming Pool Master Key.

2.0 Registration Process

The registration is carried out by the SPRA. It performs the following operations:

- 2.1 Card Operations
    - 2.1.1 Create/Update User Registration
    - 2.1.2 Create Guest
    - 2.1.3 Create Front Desk Card
    - 2.1.4 View Information of a user from user card
- 2.2 Database Operations
    - 2.2.1 View Information from database (Registration or Daily Log)
    - 2.2.2 Update Daily Log
- 2.3 System Operations
    - 2.3.1 Database connection Settings
    - 2.3.2 Edit Slots

2.1 Card Operations

2.1.1 User Registration

The User Registration consists of writing the required data into the card by the SPRA in order to register the user for usage of the swimming pool. After the successful completion of the registration, the database is updated with the new user's details.

The User Registration requires the following:

(I) Authenticate the SPRA card with User card.
(II) Check if the Swimming Pool Files exist or not:

If not:

- Create files 6F00, 6F02 & 6F03
- Write Per Card Swimming Pool Key in 6F02.
- Write the Swimming Pool User Info in 6F03 as mentioned by the User.

Else:

- Authenticate with Swimming Pool Key to verify a valid swimming Pool User.
- Update the information in 6F03.

(III) After a person is successfully registered as a Swimming Pool member, the Registration database is updated and an entry is made in the database for the current registration. If the user was previously also registered as a Swimming Pool Member, the database would have multiple entries for that member. This database is referred to as the Swimming Pool Registration Database.

2.1.2 Create Guest

The Create Guest operation is used to create a Guest Card for a Swimming Pool User who is not issued an IITK smart ID from the institute. SPRA will have some black cards which will be used to create Guest Cards for such users.

The Guest will be asked to fill in the details which will be written in the Elementary File 3F05 and 3F07 under the Master File 3F00, as is done is the IITK smart ID. However, in the Create Guest Operation, the Swimming Pool Data is not written in the Guest Card. For writing the Swimming Pool data, we need to use the Create/Update User Card Operation.

2.1.3 Create Front Desk Card

This operation is used to create a Front Desk Card to be used at the Front Desk to authenticate the User Card and to perform any updates on them. This card has the Swimming Pool Master Key in EF 7F02 under the DF 7F00. The Swimming Pool Master Key would be read from the SPRA card on providing the correct password and is written onto the FD Card.

2.1.4 View Information of a user from user card

This operation is used to extract the personal information of a User from his IITK smart ID. The information consists of his Name, Roll No. /PF No., Department, Type, Home Address, Home Phone, etc. This information is present in the Elementary Files EF5 and EF7 under the Master File 3F00. The Swimming Pool Registration Information, if available, is also displayed.

2.2 Database operations

2.2.1 View Information from Database

In the Swimming Pool Application, we maintain two different Databases:

(a) Swimming Pool Registration Database
(b) Swimming Pool Daily Log Database

Both the databases will be stored on the central server. The Registration database will be updated each time a new member is registered in the Swimming Pool and the Daily Log Database will be updated at the end of the day using a USB mass storage device (from the Front Desk PC to the central server using the Registration PC).

The **Swimming Pool Registration Database** holds the following attributes:

Serial No.: This field holds the serial number of the registration entry.

Name: This field holds the name of the user entered during the registration process by the SPRA.

ID: This field holds the Barcode ID of the user.

Type: This field holds the type of the user. This can be Student, Staff etc.

Swim User Type: This field holds the type of the user entered during the registration process by the SPRA. This can be Limited/Regular (L/R).

No. of slots (available only for ltd user): This field holds the number of slots available to the user as entered during the registration process by the SPRA. Only limited users are allotted a number of slots. Hence, the number of slots available will be available only for the limited users.

Slot No.: This field holds the slot number selected by the user as entered during the registration process by the SPRA. This field is valid only for the Regular Swim Users. The slot number and their timings are read from the Slot Configuration file and can be edited using the edit slots operation.

No. of months (Validity): This field holds the number of months that the user's account will be valid as entered during the registration process by the SPRA. This field is also valid only for the Regular Swims User.

Date and Time of Creation: This field holds the date and time of registering the user as a Swimming Pool Member.

Valid Till: This field holds the date till which the card is valid.

Money Collected: This field holds the amount that was collected from the User in order to register him as a Swimming Pool User.

Emergency Info: The next 4 fields are used to store the emergency information i.e. blood group (of the member), Contact No., Contact Person, Contact Address (of the person to be called in case of an emergency).

By entering the primary key of the search (search parameters), the SPRA will display all the registration information available in the database according to that primary key.

We can have multiple entries corresponding to a single user depending on the number of times the user is registered in the Swimming Pool.

The **Swimming Pool Daily Log Database** holds the following attributes:

Serial No: This field holds the serial number of the log.

Name: This field holds the name of the user

ID: This field holds the Roll No. /PF No. of the user.

Type: This field holds the type of the user. This can be Student, Staff etc.

Entry Time: This field holds the entry time as recorded by the front desk.

Exit Time: This field holds the exit time as recorded by the front desk.

Slot No.: This field holds the Slot No. in which the entry/exit took place.

Entry Date: This field holds the entry date as recorded by the front desk.

2.2.2 Update Daily Log

This operation is used to update the daily log collected on a day from the Front Desk onto the central server. The Daily Logs are transferred to the Registration PC using a memory stick from where the Daily Log Database can be updated with the logs of the that particular day. This operation reads the logs stored in the log files (in .txt format) and then updates the database adding these logs into the Daily Log Database.

2.3 System Operations

2.3.1 Database Connection Settings

This operation is used to change the connection settings for the database at the central server. Using this operation, the server settings can be changed or modified. This information is stored in a configuration file and is automatically read when no information regarding the database connection is mentioned.

2.3.2 Edit Slots

This Operation is used to change the slot configuration file in case the timings of a particular slot have been changed or in case a particular slot has been closed. This information is stored in the slot configuration file and is read while writing the database entry for registration of a particular user.

3.0 Front Desk Operations

In the front desk operations, the Swimming Pool Front Desk Attendant would supervise the entry/exit of Swimming Pool Members.

3.1 Procedure

When a Swimming Pool Member enters the pool, he/she will insert his/her IITK smart card registered for the swimming pool into the readers attached to the Front Desk PC. At this time, the Front Desk Card authenticates the User Card and vice versa in order to be able to update the information stored in the EF 6F03 containing the Swimming Pool Member Data. The application checks for the slot number or the number of swims left for the member (depending whether he is a regular member or a limited swims member). On successful validation of the information stored in the card, the member will see his/her name on the list of recent members and know that he/she has been authorized to enter the pool. If the member is a limited swims member then the Swimming Pool verification program would decrement the number of swims for the member using the Swimming pool Key (a derived key of which is also present in the EF2 file under DF 6F00). This is the only case in which the Verification Program changes any value of the 3 bytes that record the pool information for a particular member.

If by mistake the member re-enters the card in the reader within the next 2 minutes, nothing will happen. But after these 2 minutes, if the card is re entered, the member will be marked as exited.

If in case a user enters the pool with some mismatch in the data, i.e. if a member comes to the pool in a slot different than what he/she had registered for, then a popup is generated, asking the Administrator to take control. If the Front Desk Attendant chooses yes, the user will be allowed into the pool and his info will be displayed accordingly. Otherwise, the user will not be permitted to enter the pool.

Here, current slot is chosen by the Front Desk Application depending upon the current time. The option for choosing slots is displayed in a drop down menu for the Front Desk Attendant to view the log for that particular slot on the current date. The Current Slot is chosen from the slot configuration file and then it’s displayed. The configuration file also has time settings corresponding to different slots regarding when the entry for a particular slot is to be started and when entry for the current slot would be stopped.

4.2 Entities

The Exit All option would be used to clear the Entry/Exit list of the slot chosen from the drop down menu. This is done to mark the exit of those members who did not mark their exit properly. The Edit Slots option would be used to change the slot configuration file in case the timings of a particular slot have been changed.

Transfer Log option will be used to transfer the log of the particular day to a storage device (can be a USP storage device or a floppy). Different logs will be maintained for different slots and all of them for a particular date will exist in a directory named after that date. These files will all be .txt files by the name of the corresponding slot. These logs would be transferred to the registration PC to update the Daily Log Database on the central server. The logs are created once a member marks his entry into the pool and is written after each member enters or exits the pool.

There would be two lists that would appear in the GUI of Front Desk. The list, on the left, would display the members who have entered and then exited the swimming pool in the slot chosen above. The other list on the right, will display 10 most recent members who have entered the pool for the current slot. The lists will have the ID no of the member, the name and the time of entry/exit. This information will be read from the card in the same way as it's read during the registration. As the members enter the pool, this list is updated.

The lower half also has 2 counters. The counter on the bottom left shows the number of person who entered the pool in that particular slot. The counter on the bottom right corner shows the number of the people who have left the pool.

4.0 Work Done

During the last semester, we were using Simputer as the smart Card Reader. We were able to successfully use the Alpar protocol to send and receive commands to the IITK smart ID. We were able to read the User Information from the Card.
We were working on the GUI part for the Font Desk application when the semester ended. We later realized during this semester that Simputer takes some time to recognize the smart Cards inserted in it. We, then, decided to use a Front Desk PC with smart card readers attached to it as a replacement to two Simputers.

In the Registration Process, we have completed the registration process of User and the Guest. The Create Guest operation has also been completed. The update User part of the registration process and the Create FD card operation has also been completed. All the database operations are working and the database can be updated and searched as per the search fields. In the System operations, the Edit slot and the Database Connection operations are also working and updating the corresponding configuration file.

In the Front Desk operations, the user can mark his entry and exit into the pool. The log files are being created correctly. The edit slot operation and the Exit All operation are also working correctly. We are currently facing some problems in the updating of user data on the Front Desk.

5.0 Future Work

The Front Desk operations that we have not been able to complete are needed to be implemented. After that, the software needs to be tested and then, it would be ready to be deployed in the Swimming Pool. The program may be altered to be used for the T=1 protocol.

6.0 References

[1] International Standard Organization, Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange. ISO/IEC 7816-4, First Edition, 1995-09-01.
[2] International Standard Organization, Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands. ISO/IEC 7816-8:1999(E).
[3] International Standard Organization, Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 9: Additional interindustry commands and security attributes. ISO/IEC 7816-9:2000(E).