Software Requirements Specification Document

Version 1.0

Design and Development of CSC based Multi-Utility System *Including Access Control and Attendance Monitoring*

Team SDET: The 'Smart' People

Prof. Rahul Banerjee (Associate Professor, CSIS Group),

Mohit Vohra (PP2 Scholar, SDET Unit)

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE

PILANI (RAJASTHAN)

FEBRUARY 26, 2007

TABLE OF CONTENTS

1. Introduction

1.1 Purpose of this Document

The purpose of this SRS document is to provide a detailed overview of our software product, its parameters and goals. This document describes the project's target audience and its user interface, hardware and software requirements. It defines how our client, team and audience see the product and its functionality.

1.2 Scope of the Development Project

The goal is to design software for a CSC based Multi-Utility System including Access Control and Attendance monitoring. In this system, a user will swipe a Java Card against the reader terminal in order to perform read transactions such as checking lab status (i.e. whether it is open for all or booked for a particular course) or write operations such as marking the attendance for a particular course. All this data that's being accessed will be stored in a central repository (database server) and will also be replicated onto a backup database server on a daily basis so that cases of data loss are minimized in case of events such as power failure or link failure.

The software must be able to perform the following operations:

1. **Identify and authenticate card:** It must be able to authenticate the card user by matching the ID no. / PSRN no. and the access code (which in turn may be generated using some cryptographic algorithm) against the values stored in the database.
2. **Check lab/room status:** It must be able to check the lab/room status by querying the database for any reservation requests made earlier. This function must be called immediately after the card has been validated and then a set of options must be offered to the user.
3. **Record user's presence:** It must be able to record the user's presence by writing the user's ID no. / PSRN no. in the corresponding database table. Thus for one swipe, two write operations will be performed: one into the central repository and other into the backup database server.
   Note: A key point to be noted here is that the card has to be swiped every

time a user is entering/ exiting the room/lab. For each swipe the time in/out will also be recorded and the total time spent in the lab will be computed by subtracting the time when user entered the lab with the time when the user came out of the lab. This will help the lab-in-charge to be aware of the time spent by the lab users even when the lab-in-charge is not physically present in the lab.

4. **Update access privileges:** The software must be able to update the access privileges onto a particular user's card and the database where the privileges themselves will be modifiable only by the system administrators (or some authorized staff members).
5. **Determine access privilege levels:** The software must be able to determine whether a particular user has been denied access from a particular lab due to some policy violation. The results of this operation will be viewable by the security officer only.

Initially we plan to implement these functionalities for the 4 SDET unit labs with an intended audience of 60 people (of which 12 are staff members and remaining are students) as part of the **Pilot Phase**. Once the Pilot Phase is successful then we plan to implement it in other labs across the institute and eventually we plan to extend the CSC based Multi-Utility System including Access Control and Attendance Monitoring to a wide variety of applications including library system, semester fee payment system, etc.

The scope of this system is not just limited to the Pilani campus only as the same mechanism can be reused in other campuses as well (Goa, Dubai and even the upcoming Hyderabad one). This system can also be implemented in the industrial sector where smart cards can take place of the Time Office system where a person sitting at the entrance notes down the time an employee entered the office and the time the person went out on break, came back and also the time when the person left the office in the evening. This scenario is prevalent in many industries today, with the notable ones being the cement, mining and other industries, although the same cannot be said of the IT companies as almost all the major software companies have already implemented smart card based access control mechanisms wherein the employee ID card doubles up as the smart card as well.

1.3 Definitions, abbreviations and acronyms

Definitions

Table 1 gives explanation of the most commonly used terms in this SRS document.

Table 1: Definitions for most commonly used terms

S.No.	Term	Definition
1	Biometric Authentication	Refers to technologies that measure and analyze human physical & behavioural characteristics for authentication purposes [1].
2	Contactless Smart Card	A second type is the contactless smart card, in which the chip communicates with the card reader through RFID induction technology (at data rates of 106-848 kbit/s). These cards require only close proximity to an antenna to complete transaction [2].
3	ISO 14443	It's a four-part international standard for contactless smart cards operating at 13.56 MHz in close proximity with a reader antenna. This ISO standard sets communication standards and transmission protocols between card and reader to create interoperability for contactless smart card products [4].
4	ISO 7810	Describes the physical characteristics of different smart cards and also the overall dimensions of the card (along with ISO 7816-2) [5].
5	ISO 7816	The basic contact smart card standard is the ISO 7816 series. These standards are derived from the identification card standards and detail the physical, electrical, mechanical, and application programming interface [5].
6	Java Card	A Java Card is a smart card capable of running programs written in Java.
7	MIFARE	It's a separate standard developed by NXP (formerly Philips Semiconductors) that closely models the ISO 14443A standard and is now widely used to develop contactless smart cards by NXP [6].

8	RFID	It's an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders [3].
9	SCOSTA	Describes the minimum support for the application using the Smart Cards. A SCOSTA compliant operating system will also be compliant to the ISO7816-4, -8 and -9 standards [7]. Primary usage of SCOSTA is in transport applications.
10	Smart Card	A smart card [2], chip card, or integrated circuit(s) card (ICC), is defined as any pocket-sized card with embedded integrated circuits

Abbreviations

Table 2 gives the full form of most commonly used mnemonics in this SRS document.

Table 2: Full form for most commonly used mnemonics

S.No.	Mnemonic	Full Form
1	ACG	Smart card distributor that's part of ASSA ABLOY Identification Technologies
2	CSC	Contactless Smart Card
3	SDET	Software Development and Educational Training
4	IPC	Information Processing Center
5	NXP	NXP (for Next eXPerience) Semiconductors is the name for the new semiconductor company founded by Philips as announced by its CEO Frans van Houten to its customers and employees in Berlin on Thursday night 2006-08-31 and to the global media early on Friday morning 2006-09-01 [8].
6	RFID	Radio Frequency Identification
7	SCOSTA	Specifications for the Smart-Card OS for Transport Applications

1.4 References

[1]. Biometric Authentication Definition. Link: http://en.wikipedia.org/wiki/Biometrics
[2]. Smart Card Definition. Link: http://en.wikipedia.org/wiki/Smart_card
[3]. RFID Definition. Link: http://en.wikipedia.org/wiki/RFID
[4]. ISO 14443 Introduction by OTI Global. Link: http://www.otiglobal.com/objects/ISO%2014443%20WP%204.11.pdf
[5]. Won J. Jun, Giesecke & Derivent (G & D). July 8, 2003. 'Smart Card Technology Capabilities'. PDF link: http://csrc.nist.gov/publications/nistir/IR-7056/Capabilities/Jun-SmartCardTech.pdf
[6]. MIFARE website. Link: http://mifare.net/about/
[7]. Specifications for the Smart-Card OS for Transport Applications (SCOSTA) PDF Link: http://www.scosta.gov.in/SCOSTA_1.pdf
[8]. NXP by Wikipedia. Link: http://en.wikipedia.org/wiki/NXP_Semiconductors
[9]. Data Replication Strategies. A White Paper by Jay Orcutt, Data Management Architect, Sun Microsystems. PDF Link: http://www.sun.com/storagetek/white-papers/data_replication_strategies.pdf
[10]. Data Replication Strategies in Grid Environments. Ewa Deelman, Information Sciences Institute, University of Southern California in collaboration with Houda Lamehamedi et al. Department of Computer Science, Rensselaer Polytechnic Institute. PDF Link: http://www.cs.rpi.edu/~szymansk/papers/ica3pp.02.pdf
[11]. A Performance Study of Three High Availability Data Replication Strategies. David J. DeWitt, Computer Sciences Department, University of Wisconsin in collaboration with Hui-I Hsiao, IBM T.J. Watson Research Center. PDF Link: http://www.cs.wisc.edu/~dewitt/includes/paralleldb/pdis91.pdf

1.5 Overview

The remaining sections of this document provide a general description, including characteristics of the users of this project, the product's hardware, and the functional and data requirements of the product. General description of the project is discussed in section 2 of this document. Section 2 gives the functional requirements, data requirements and constraints and assumptions made while designing the multi-utility system. It also gives the user viewpoint of product use. Section 3 gives the specific requirements of the product. Section 3.0 also discusses the external interface requirements and gives detailed description of functional requirements.

2. Overall Description

2.1 Product Perspective

The product will run as a component of the smart card reader-writer device. The product does not require use of a pointing device or keyboard but it does require a small keypad with numbers 1-9 where each number represents a particular functionality that the user can avail. For example, by pressing 1, a faculty member (staff) can reserve 2 labs of IPC unit for 2 hours.

Figure 1 shows the layout for SDET Unit's Microsoft Lab with the smart card reader-writer placed next to the lab entrance.

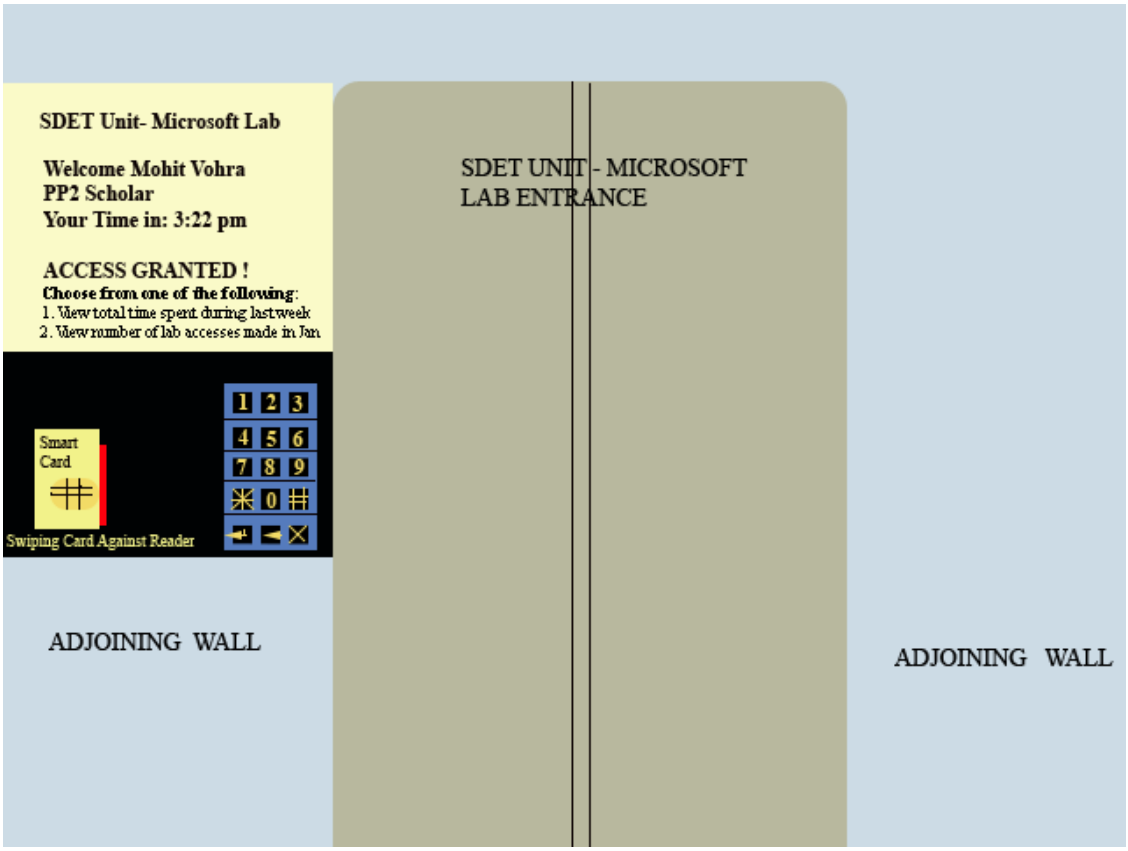

Figure 1: SDET Unit Media Lab using Smart card based System

Here the user will have to swipe his/her smart card against the reader-writer terminal and once the terminal identifies the card user by matching the cryptographic key generated by the software with the one generated by the card, the

welcome message is displayed to the user. Next, the software inside the terminal will check whether the student has access permission for the lab or not, i.e. it will check whether the student has been denied access due to some official reason or not. If the student has been denied access, then the software will send the message "Access Denied" onto the screen. Otherwise an "Access Granted" message will be displayed and the student can then enter the lab and access the resources.

In addition to the welcome message, each user will be able to perform a limited set of read-write operations. Figure 1 shows the options that will be visible for the student who's working in the Microsoft Lab.

The above mechanism can be explained in a better manner with the help of the following figure (Figure 2).

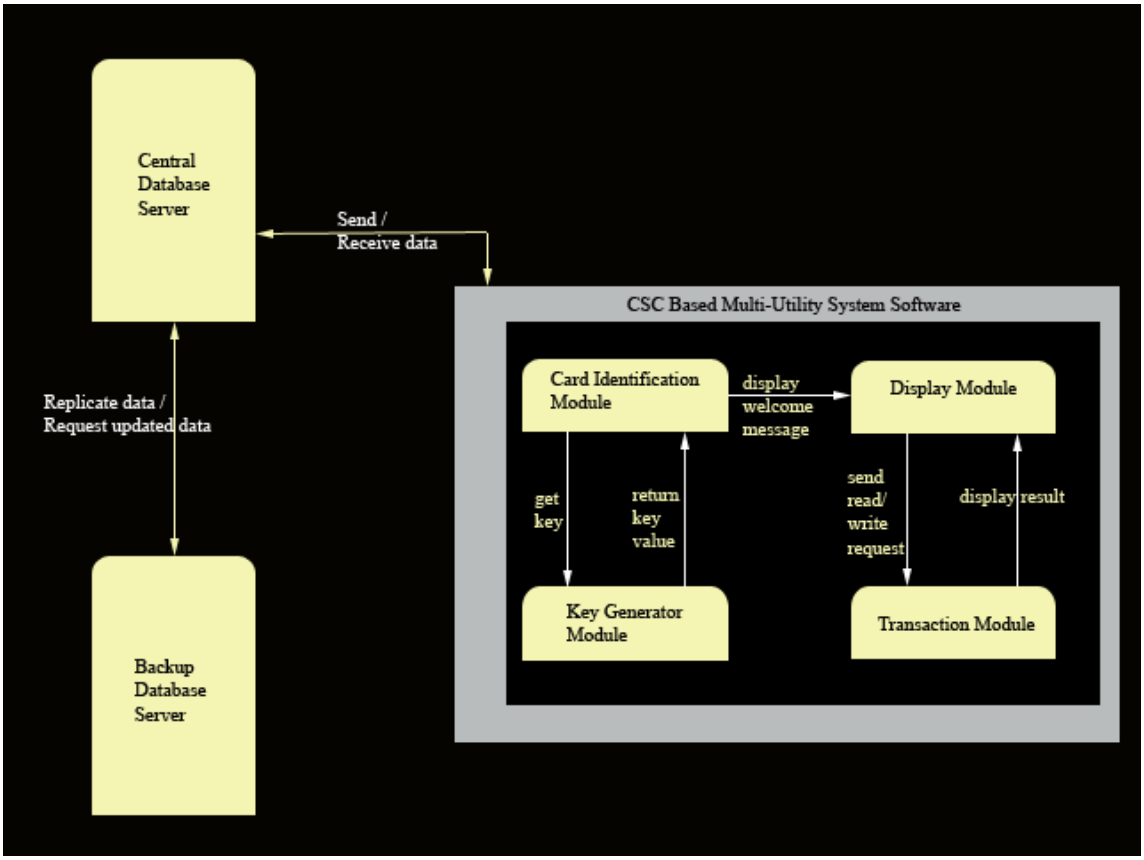

Figure 2: Block Diagram of the CSC based Multi-Utility System including Access Control and Attendance Monitoring

Here the CSC based Multi-Utility System including Access Control and Attendance

Monitoring has been depicted as a Black box that in turn contains four major modules:

1. Card Identification
2. Key Generator
3. Display
4. Transaction

Upon swiping the card against the reader-writer device, the **Card Identification Module** will authenticate the card user by matching the ID No. / PSRN No. and the access code against the values stored in the central database server.
The Card Identification Module in turn will call the **Key Generator Module** in order to obtain the key. The **Key Generator Module** will compute the key using some cryptographic algorithm and will return the value to the Card Identification Module.

Once the card has been successfully identified the user will see a welcome message on the display screen similar to the message displayed in Figure 1 above. The Card Identification Module will thus send the card user's name to the **Display module** that will in turn print the welcome message onto the screen. Depending on the operation requested by the user (for example a faculty member may want to know how many students are present in the SDET Unit's Microsoft Lab or may want to reserve a room), the Display Module will call the **Transaction Module** with the respective operation.

Here I have defined a transaction as a simple read /write operation where the data to be read / written may differ with each request. Thus a staff member trying to reserve a room for a test can be considered as a write transaction whereas a staff member trying to see number of students taking that test in the room on that particular date will be considered as a read transaction. The **Transaction Module** will thus process the read/write transaction and display the appropriate message back to the display screen by passing the message to the Display Module.

In addition to the four modules, a **Central database server** and a **Backup database server** will also be used in order to read/write data onto the repository. The central database server will periodically update the Backup database server so that in case of server failure it can restore the data by retrieving the records stored

in the Backup database server's tables. I have enclosed the four modules in a grey rectangle in order to indicate that these 4 modules comprise the major components of the CSC based Multi-Utility System software. And by showing a single arrow between the software and the central database server, I wish to convey the point that at a given point of time only one module within the software will communicate with the server database. That is, the card identification module and the transaction modules will not access the database at the same time as first a card has to be authenticated, following which the transactions can be processed.

2.2 Product Functions

The product should be able to perform the following operations:

1. It must be able to authenticate the card user by matching the ID no. / PSRN no. and the access code against the values stored in the database.
2. It must be able to check the lab/room status by querying the database for any reservation requests made earlier.
3. It must be able to record the user's presence by writing the user's ID no. / PSRN no. in the corresponding database table. Thus for one swipe, two write operations will be performed: one into the central repository and other into the backup database server. For each swipe the time in/out will also be recorded and the total time spent in the lab will be computed by subtracting the time when user entered the lab with the time when the user came out of the lab.
4. The software must be able to update the access privileges onto a particular user's card and the database where the privileges themselves will be modifiable only by the system administrators (or some authorized staff members).
5. The software must be able to determine whether a particular user has been denied access from a particular lab due to some policy violation. The results of this operation will be viewable by the security officer only.

2.3 User Characteristics

The goal is to design software for a CSC based Multi-Utility System including Access Control and Attendance monitoring for different users. These user types are listed below as follows:

1. Student
2. Staff
3. Student cum Staff
4. Group Leader
5. Dean/Unit Chief
6. Deputy Director
7. Director
8. Vice-Chancellor
9. Security Officer
10. Medical Officer
11. Chief Medical Officer
12. Chief Accountant

As one can see from the list, each user will have different educational background and expertise level in using the system. Our goal is to develop software that should be easy to use for all types of users, including the Security Officer. Thus while designing the software one can assume that each user type has the following characteristics:

- The user is computer-literate and has little or no difficulty in using smart card to access information such as room status.
- In order to use the smart card it is not required that a user be aware of the internal working of a smart card but he/she is expected to know what happens when the card is swiped against the reader.

2.4 General Constraints, Assumptions and Dependencies

The following list presents the constraints, assumptions, dependencies or guidelines that are imposed upon implementation of the CSC based Multi-Utility System including Access Control and Attendance Monitoring software:

- The software has to be integrated onto the reader-writer terminal that in turn has an extremely small form factor and has support for limited capability APIs only.
- Due to the small form factor, only limited graphics can be supported on the display screen.
- There are no memory requirements
- The product must have a user friendly interface that is simple enough for all types of users to understand.
- Response time for loading the software and for processing a transaction should be no longer than five seconds.
- A general knowledge of basic computer skills and of basic working of smart card based system is required to use the product.
- The central database server and backup database servers should be updated regularly. This updating and replication of data from central database server to the backup database server can introduce additional latency in the working of the system.
- The replication of data from central to the backup server has to be Asynchronous as Asynchronous solutions also provide a greater amount of protection by extending the distance between the primary and secondary locations of the data. Increased distances can provide protection from local events as the loss of a power grid, as well as natural disasters such as earthquakes and hurricanes [9]. Interesting work in this regard has been done by University of Wisconsin, Madison [11], University of Southern California and Rensselaer Polytechnic Institute, NY [10] scholars.

2.5 Apportioning of requirements

The CSC based Multi-Utility System (including Access Control and Attendance Monitoring) is to be implemented in the following three phases:

i. **Pilot Phase:** Here the smart card based multi-utility system including access control and attendance monitoring will be implemented in the 4 SDET unit labs with the help of 60 smart cards and 4 reader-writers. Initially we will be providing access privileges for three types of users: student, staff and student cum staff as they will be ones most involved in this phase.

ii. **Institute wide deployment:** Following the successful completion of the pilot phase, we plan to deploy the same across the institute (including the BITS Goa, Dubai and the upcoming Hyderabad campus as well). Biometric authentication will also come into the picture in this phase only, wherein small fingerprint sensors will be placed next to the server class machines inside the SDET Unit labs to start with.

iii. **Extension of smart card based multi-utility system to other applications:** In the future we can have a single student smart card for example serving different purposes like purchasing a textbook at the BITS Co-operative store or paying the semester fees, an application that will really boost the utility value of the smart cards.

Here the same functionalities will be implemented in each phase; the only difference will be the number of transactions being carried out and the scale of implementation.

3. Specific Requirements

3.1 External Interface Requirements

The following list presents the external interface requirements:

- The product requires very limited graphics usage with just a simple keypad for taking the user input.
- The product does not require usage of sound or animation. The hardware and operating system requires a screen resolution not more than 320 x 240 pixels (owing to the small form factor).
- Sound is not an essential feature but it can be considered for future variants of the system wherein the user will be greeted by his name as he swipes his card against the reader-writer terminal.

3.2 Detailed Description of Functional Requirements

Table 3 shows a template that I'll be using to describe functional requirements for three types of users: student, staff, student cum staff as one can easily deduce the functional requirements for other user types with this template.

Table 3: Template for describing functional requirements

Purpose	A description of the functional requirements and its reasons
Inputs	What are the inputs; in what form will they arrive; from what sources can the inputs come; what are the legal domains of each input.
Processing	Describes the outcome rather than the implementation; includes any validity checks on the data, exact timing of operation (if needed), how to handle unexpected or abnormal situations
Outputs	The form, shape, destination and volume of output; output timing; range of parameters in the output; unit of measure of the output; process by which output is stored or destroyed; process for handling error message produced as output.

3.2.1 Functional Requirements for Student Welcome Screen

Table 4 gives the functional requirements for Student Welcome Screen.

Table 4: Functional Requirements for Student Welcome Screen

Purpose	This screen thus provides information specific to each student upon the successful identification of the ID no. and the access code with the values stored in the central database server.
Inputs	A student can view a page of information by choosing from one of the options given on the welcome screen. Selection is performed with a simple keypad.
Processing	The menu responds to selections by displaying a page containing the pre-defined text requested information.
Outputs	Output consists of a screen of information specific to a student. For example, as shown in Figure 1, upon choosing option '2' in the welcome menu, a student may be able to see the number of visits he made to the Microsoft lab in the last month.

3.2.2 Functional Requirements for Staff Welcome Screen

Table 5 gives the functional requirements for Staff Welcome Screen.

Table 5: Functional Requirements for Staff Welcome Screen

Purpose	This screen provides information specific to each staff member.
Inputs	A staff member can view a page of information by choosing from one of the options given on the welcome screen. Selection is performed with a simple keypad.
Processing	The menu responds to selections by displaying a page containing the pre-defined text requested information.
Outputs	Output consists of a screen of information specific to a staff member and the students studying under him. For example, upon choosing option '4' in the menu displayed on the welcome screen, a faculty member may be able to see the number of students who have appeared for the CP 1 test being held in room 2201.

3.2.3 Functional Requirements for Student cum Staff Welcome Screen

Table 6 gives the functional requirements for Student cum Staff Welcome Screen.

Table 6: Functional Requirements for Student cum Staff Welcome Screen

Purpose	This screen provides information specific to each student cum staff.
Inputs	A student cum staff can view a page of information by choosing from one of the options given on the welcome screen. Selection is performed with a simple keypad.
Processing	The menu responds to selections by displaying a page containing the pre-defined text requested information.
Outputs	Output consists of a screen of information for student cum staff in terms of personal information with respect to the courses where the user is a student and information with respect to the students where the user is a staff member. For example, if a member of Economics group is also studying Object Oriented Programming and is also taking the Security Analysis and Portfolio Management course, then the member will be able to see data related to students taking the course Security Analysis and Portfolio Management and also see data relating to the course Object Oriented Programming in which he is a student.

3.3 Performance Requirements

- The software is designed for the smart card reader-writer terminal and cannot run from a standalone desktop PC.
- The software will support simultaneous user access only if there are multiple terminals.
- Only textual information will be handled by the software. Amount of information to be handled can vary from user to user.
- For normal conditions, 95% of the transactions should be processed in less than 5 seconds.

3.4 Logical Database Requirements

Figure 3 shows the E-R diagram for the entire system.

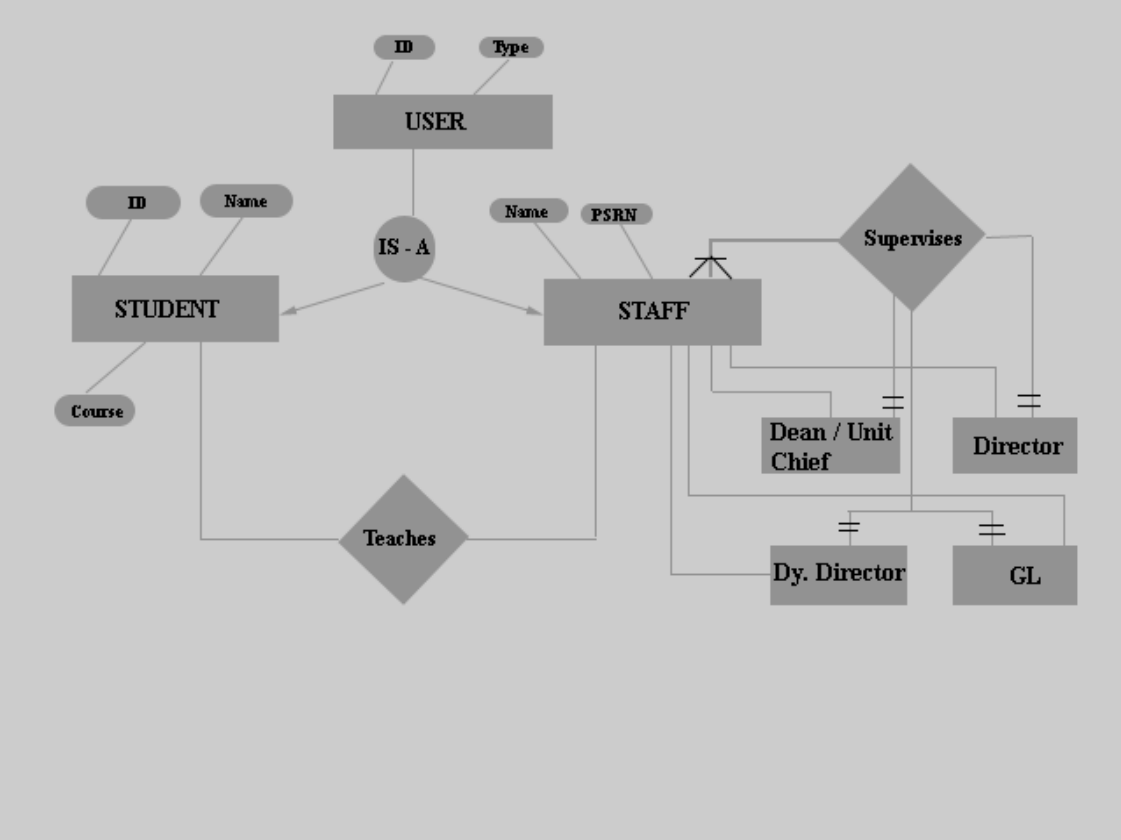

Figure 3: E-R Diagram for the CSC Based Multi-Utility System (including access control and attendance monitoring)

3.5 Quality Attributes

The product is target towards a wide variety of users such as Student, staff, student cum staff, etc. The product must load quickly and work well on a variety of terminals. It must also tolerate wide variety of input possibilities from a user, such as incorrect responses or unforeseen keystrokes.

3.6 Other Requirements

None at this time

4. Change History

20070226	Version 1.0 – Initial Release

5. Document Approvers

SRS for CSC based Multi-Utility System (including Access Control and Attendance Monitoring) approved by:

_____

(Rahul Banerjee)
Unit Chief, SDET
Date: 26.2.2007