



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA



Software Requirements Specification: Next Gen ATM COS 301: Group 7

Richard McFadden
17026662

Brian Ndung'u
15322913

Aeron Land
17140634

Sisa Khoza
15034993

Adrian le Grange
17056782

22 February 2019

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 2 |
| 1.1 | Vision and scope | 2 |
| 1.1.1 | Background | 2 |
| 1.1.2 | Vision | 2 |
| 1.1.3 | Business need | 2 |
| 1.1.4 | Scope | 2 |
| 2 | User Characteristics | 3 |
| 3 | Functional Requirements | 4 |
| 3.1 | Authentication | 6 |
| 3.1.1 | Data Connection | 6 |
| 3.1.2 | NFC as one method of authentication | 6 |
| 3.1.3 | Encryption of data | 6 |
| 3.2 | Registration | 7 |
| 3.2.1 | Registration of clients | 7 |
| 3.2.2 | Registration of vendors | 7 |
| 3.2.3 | Registration of admin users | 7 |
| 3.3 | Transactions | 7 |
| 3.3.1 | Deposits | 7 |
| 3.3.2 | Withdrawals | 7 |
| 3.3.3 | Settling accounts | 7 |
| 3.3.4 | Balance Enquiry | 7 |
| 3.4 | Auditing | 8 |
| 4 | Quality Requirements | 9 |
| 4.1 | Reliability | 9 |
| 4.1.1 | Internet Connection | 9 |
| 4.1.2 | Connectivity | 9 |
| 4.1.3 | Logging | 9 |
| 4.2 | Security | 9 |
| 4.2.1 | Authentication | 9 |
| 4.2.2 | Sessions | 9 |
| 4.3 | Performance | 9 |
| 4.3.1 | Response Time | 10 |
| 4.3.2 | Throughput | 10 |
| 4.4 | Cost | 10 |
| 4.4.1 | ATM's | 10 |
| 4.4.2 | System | 10 |
| 5 | Trace-ability Matrix | 10 |

1 Introduction

1.1 Vision and scope

1.1.1 Background

FNB wishes to gain a competitive edge in an over saturated market by developing next-gen ATM's that aim at changing the way clients interact with the system. These changes involve reducing waiting and interacting times with the ATM. The system has to use NFC technology and two-factor authentication to accomplish the following transactions: withdraw, deposit and viewing of balances.

1.1.2 Vision

Our vision is to change the way clients view ATM's and create a digital ATM from which clients can do their banking. Tasks like withdrawal, balance enquiry and depositing of cash will all happen either on or through our system. We intend to eliminate the need for queues and outdated ATM interfaces by incorporating new technology and processes that are becoming standard in our everyday lives like Peer-to-Peer mobile payments, NFC, biometric authentication and mobile applications. These technologies allow us to give the client instant service.

1.1.3 Business need

To future proof and digitize the way clients interact with ATM's. In order to provide a more interactive, convenient and means of performing ATM related actions, while reducing overhead costs involved with installing and maintaining ATM's.

1.1.4 Scope

The proposed system will consist of a mobile application with two portals used by clients and vendors. The client's portal will enable them to deposit cash, withdraw cash, view balance and request a balance statement. The vendor's portal will enable them to pay or receive cash from clients in place of the bank. Communication between the client and vendor will be facilitated through wireless technology with it being additionally supplemented with another layer of authentication. The system will provide a means of storing client information as well as logging transaction and access history for the purpose of auditing. The System must be completed withing 7 weeks.

2 User Characteristics

- **Clients** - the target audience of the system. They should have access to a smartphone and should be the bank's client. They will interact with the system in order to be able to access their account, verify transactions, withdraw cash, deposit cash and request a balance statement using the app.
- **Vendors** - this consists of both individuals and ATM's. They would interact with the system to pay clients or receive deposits from clients on behalf of the bank. Vendors would need to settle the account with the bank to keep track of what is owed to the bank and what is owed to the vendor.
- **System Administration** - the supervisor of the system. System Administration should be an employee of the bank. They will interact with the system in order to be able to register clients and vendors, settle accounts with vendors and perform auditing.

3 Functional Requirements

The section of the document specifies the functional requirements for the project in terms of use cases.

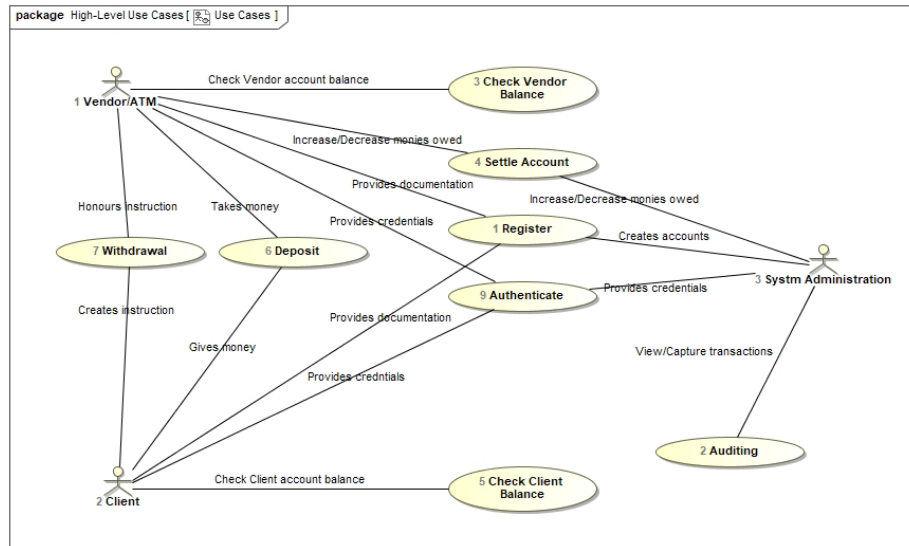


Figure 1: System Overview

The system will consist of subsystems that will integrate and communicate with each other. These subsystems have been divided into transactions, authentication, auditing and registration.

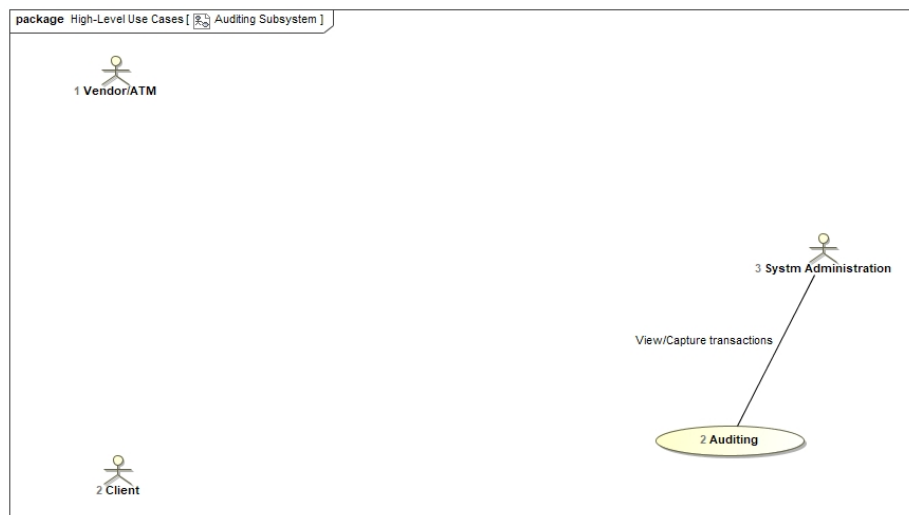


Figure 2: Auditing Subsystem

The Auditing subsystem allows for the viewing, downloading, auditing and querying of the logs. This is done by System administration.

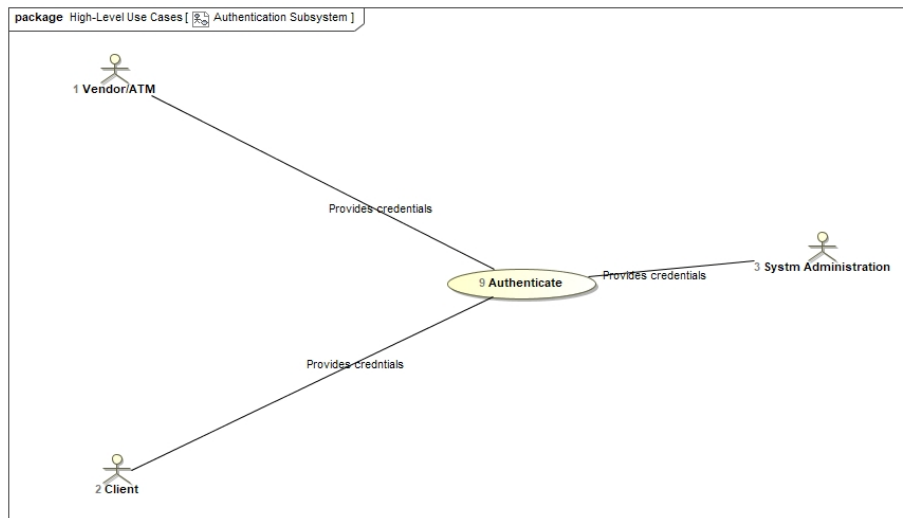


Figure 3: Authentication Subsystem

The client, vendor/ATM and the system administration will need to log in to the system and use any of the registered authentication methods. Authentication will also need to take place with each transaction that takes place.

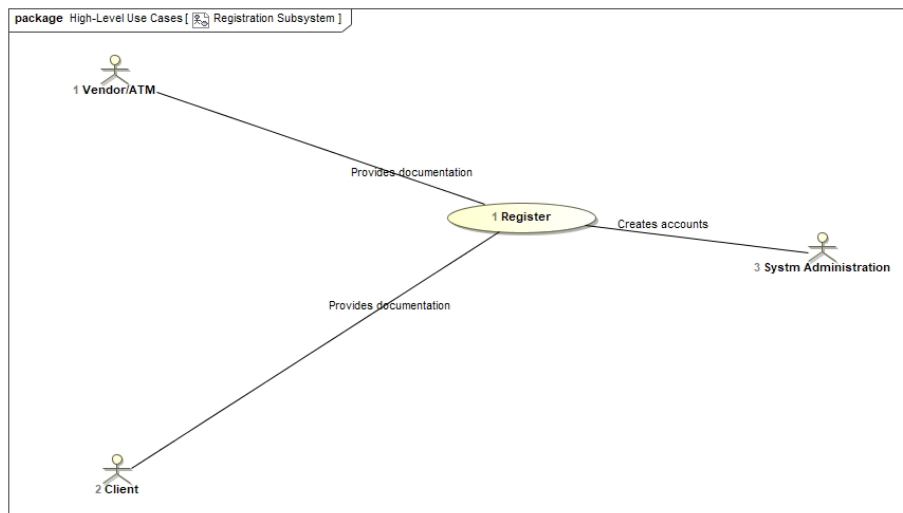


Figure 4: Registration Subsystem

The client must register to be able to use our system. The system administration is responsible for creating and enabling the accounts.

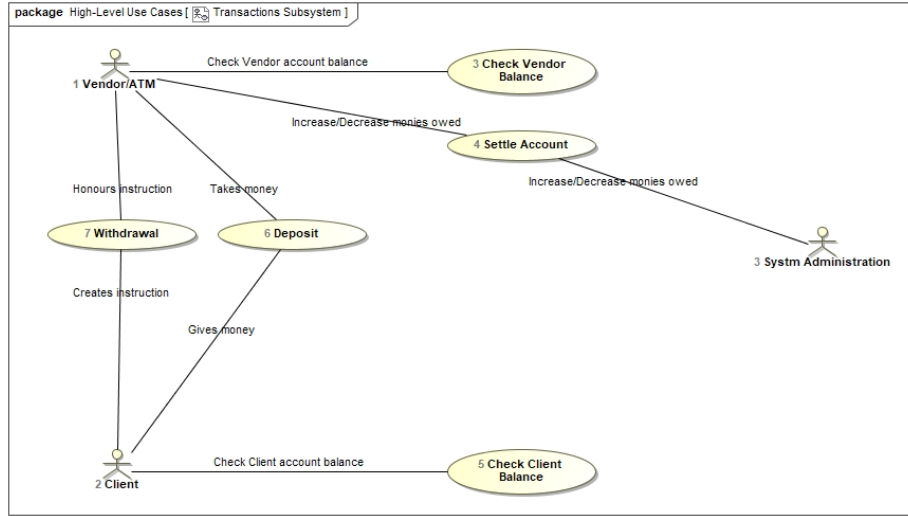


Figure 5: Transaction Subsystem

The client needs to be able to view balances, withdraw, and deposit cash from the system. This is accomplished using the vendors. The vendor needs to be able to view its balances, this includes what is to be paid to the bank and what the bank owes, as well as receive and present cash to the client on behalf of the bank. The system administration must be able to settle accounts with the vendors.

3.1 Authentication

3.1.1 Data Connection

The mobile app will primarily communicate over WiFi/cellular data. Should neither be available then the app will fallback on using USSD on a GSM network because 8 million smartphone users in South Africa cannot afford data.

3.1.2 NFC as one method of authentication

Currently bank cards have NFC capabilities that is used as a way of authenticating small transactions. This system will use NFC as one of the two factors for authentication. To cater for the 25 percentage of client that do not have a cellphones with NFC capabilities, NFC tags (or stickers) will be issued on demand, that the client can stick on their cellphone to provide this functionality. The client's NFC device ID is then bound to their account upon registration.

3.1.3 Encryption of data

Given the sensitive nature of data being sent/received, encryption of transmitted data between client and server will be needed. The AES and RSA encryption algorithms will be used to ensure private end-to-end connections.

3.2 Registration

All users of the system will be required to register their NFC enabled smart-phones or NFC tags with the system. Users registering on the system will need to provide a photo to identify themselves.

3.2.1 Registration of clients

A client can open an account from their phone but to activate it they have to visit a branch in order for an admin user to bind a single NFC device to the client's account.

3.2.2 Registration of vendors

Vendors follow the same method as clients described above but are subject to any recruitment policies and checks required by the bank. (e.g background checks)

3.2.3 Registration of admin users

Admin users can register or remove other admin users.

3.3 Transactions

Before any transaction can be made the client, vendor or both has to be authenticated using two factor authentication.

3.3.1 Deposits

Deposits can be made by the client to a vendor. The deposit would be logged on the vendors account as an amount that needs to be transferred to the bank.

3.3.2 Withdrawals

When a client wants to make a withdrawal, he/she would be able to do so on their device. They can then go to any vendor to collect their withdrawn cash by authenticating themselves.

3.3.3 Settling accounts

Vendors would have the functionality to be able to settle their account with the bank. If they are owed by the bank they can select their preferred method to receive the owed amount. If the vendor owes the bank they can make an electronic payment to the bank or make a deposit at another vendor.

3.3.4 Balance Enquiry

- **As Vendor** - Vendors can do a balance enquiry that will show the amount owed to them or the amount due to the bank. This balance is based on the transactions done as a vendor.
- **As Client** - The client will be able to do a balance enquiry as they currently would on an ATM. This balance is that of their personal account(s).

3.4 Auditing

This subsystem will keep track of all actions done by all users of the system. All audit logs will have a timestamp associated with the action performed, along with the users involved in the process.

4 Quality Requirements

4.1 Reliability

This subsection describes the reliability of the system that applies to the project at hand.

4.1.1 Internet Connection

The system is designed to allow users to make use of all functionality with or without internet connection.

4.1.2 Connectivity

The system will implement a periodic connection checker to test check whether or not the device has an internet connection.

4.1.3 Logging

The system will log all transactions to a database. The system must encrypt all the data send from and to the database.

4.2 Security

This subsection describes the security requirements that apply to the project at hand. It specifies how the system will ensure that all transactions will take place securely and how personal info will be stored and used.

4.2.1 Authentication

- **Clients-** The system requires all clients to identify themselves when they withdraw,pay or deposit money by means of the registered authentication methods.
- **Vendors(Business/ATM)-** The system will require authentication and identification from the user before transactions by any vendor can take place.
- **Admin-** The system requires the admin to authenticate and identify themselves when working with sensitive information. Authorization on this level is of a higher class because of the nature of the data that is being processed.

4.2.2 Sessions

The system will create, maintain, log and destroy sessions based on the client's activity. All session information must be stored to the database.

4.3 Performance

This subsection describes how the system performs and the means of performance improvements when using the system.

4.3.1 Response Time

Interaction and Transactions will appear to take effect immediately in the system. The system should not take longer than one second to respond.

4.3.2 Throughput

The system will cater for clients with slower connections and the amount of data send through depending on the network the client is connected to. The system will not send large amounts of data on slower connections.

4.4 Cost

This subsection describes the way that the system will reduce costs based on the current employed system and roughly what the new system will cost.

4.4.1 ATM's

The system will reduce ATM costs (maintenance, etc) by more than 30% in the first year. Once ATM's are deprecated the system will no longer have to maintain ATM's.

4.4.2 System

The system will cost no more than 45% of the existing system's costs to be implemented. After implementation the system should save about 30% on costs and increase this number by 5% every second year.

5 Trace-ability Matrix

1. Auditing
 - 1 Auditing
2. Authentication
 - 1 Authenticate
3. Registration
 - 1 Register
4. Transaction
 - 1 Check Vendor Balance
 - 2 Settle Account
 - 3 Deposit
 - 4 Withdrawal
 - 5 Check Client Balance

| Functional Cluster | Functional Description | System Requirements | Functional Subsystem Identified |
|--------------------|---|------------------------------|---------------------------------|
| Auditing | This subsystem will log all transactions as well as accesses on and to accounts | R1.1 | Auditing Subsystem |
| Authentication | The subsystem will handle identifying users, and applying specific rights to said account | R2.1 | Authentication Subsystem |
| Registration | This subsystem will oversee the capture of data for users/vendors, so well as provide their accounts | R3.1 | Authentication Subsystem |
| Transaction | This subsystem will have duties related to transacting on the system. It will provide functionality for CRUD operations on client/vendor accounts | R4.1, R4.2, R4.3, R4.4, R4.5 | Transaction Subsystem |

1

| | Auditing | Authentication | Registration | Transaction |
|------|----------|----------------|--------------|-------------|
| R1.1 | X | | | |
| R2.1 | | X | | |
| R3.1 | | | X | |
| R4.1 | | | | X |
| R4.2 | | | | X |
| R4.3 | | | | X |
| R4.4 | | | | X |
| R4.5 | | | | X |

2

¹Figure 6.1 - Functional clusters and functional subsystems

²Figure 6.2 - Requirements to subsystem traceability matrix