COS301

ROUND 1 – SYSTEMS REQUIREMENTS SPECIFICATION

February 21, 2019

Group 8

Graeme Coetzee	u17005168
Reinhardt Eiselen	u14043302
Andrew Jordaan	u16033796
Herbert Magaya	u17079544
Joan Mwaniki	u16159323

Contents

1 Introduction **1**
1.1 Purpose . . . 1
1.2 Scope . . . 1
1.3 Glossary . . . 2
1.4 Abbreviations . . . 2
1.5 References . . . 2
1.6 Overall review . . . 2

2 User Characteristics **3**
2.1 Existing Client . . . 3
2.2 New Client . . . 3
2.3 Limited Access Client . . . 3
2.4 Technician . . . 3

3 Functional Requirements **3**
3.1 UML Diagrams . . . 4

4 Quality requirements **7**
4.1 Performance . . . 7
4.2 Reliability . . . 7
4.3 Security . . . 7
4.3.1 Authentication . . . 8
4.3.2 Authorization . . . 8
4.3.3 Data Security . . . 8
4.4 Scalability . . . 8
4.5 Flexibility . . . 9
4.6 Auditability . . . 9
4.7 Usability . . . 9

5 Trace-ability matrix **10**

References **10**

1 Introduction

1.1 Purpose

The purpose of this document is to present an overview the proposed next generation ATM.[10] To elicitate it's requirements, along with more information on the system parameters and goals. To describe the target audience, user interface, and high-level hardware and software requirements for the proposed system. This document is intended for both FNB, the stakeholders, and the developers who will implement the system.

1.2 Scope

The proposed product is a next generation ATM system intended to completely replace, or possibly through slow integration to eventual complete assimilation, the current ATM system in use by FNB. The main aim and objective is to improve the general FNB ATM customer's overall experience of using an ATM. Improvement being in terms of security, convenience, and speed.

Focus is put on speeding up the process of withdrawing money and depositing money at an ATM, and increasing the security of the customer during and post transaction by improving on the authentication process. This will mainly be achieved through the use of NFC[13] and mobile technology[1] for the authentication of the process.

The product will not lose any of the current ATM functionality, and will still support card based operation, however the intention is to encourage customers to make use of their own personal mobile devices instead of relying on cards provided by the bank.

Main uses of the product include to withdraw, deposit money from the ATM and check balances. Benefits of the product include more secure transactions, deposits and withdrawals. Reduced queuing times will be achieved due to quicker and almost instant authentication process during withdrawals and deposits. A consequent benefit of the prior includes safety, as petty theft taking place during ATM transactions is a reality in South Africa.[17] So more than just speeding up the process we wish to add alternatives to cash withdrawals.

The goal of the product is to make the life of an FNB customer easier and safer when they need to interact with an ATM.

1.3 Glossary

Stakeholders	Any person who has an interest in the project who is not developer.[5]
Database	Collection of information stored in a sorted matter.[3]
Biometrics	The application of statistical analysis to biological data.[14]
QR Code	is a type of barcode that contains a matrix full of dots that can be scanned and read by using special software[2]
QR Code reader	a device/smartphone that has a camera and compatible software that decodes the QR code into a string of characters that contain requested information.
Card PIN	a number allocated to an individual and used to validate electronic transactions.[8]
Chatbot	a computer program designed to simulate conversation with human users, especially over the Internet.[12]

1.4 Abbreviations

NFC	Near-field Communication
FNB	First National Bank
QR code	Quick Response code
ATM	Automatic Teller Machine

1.5 References

In-line citations are used throughout this document. The complete list of references is provided at the end of the document.

1.6 Overall review

The next part of the document, the Overall Description section gives an overview of the functionality of the product in more details. It describes how the product interfaces will work along with the functions that will be performed by the product. This section gives context to forming the functional and technical requirements deemed necessary for the system. The third section of this document is focused on Requirements Specification and the target audience of this section are the developers that will be working on this project. To help give a better clear understanding of what the project requirements are, use cases will be provided to showcase the interaction between the system and its users.

2 User Characteristics

2.1 Existing Client

An Existing customer wants to utilize a bank service and they either don't have the time to go into a branch, or it is inconvenient to do so. Services include withdrawing or depositing cash, verify FNB Online Banking and the FNB Banking App, and various cardless services

2.2 New Client

A new customer will use the ATM to apply for an account and possibly register for Cellphone Banking

2.3 Limited Access Client

This customer does not have access to online or cellphone banking and wants to view their account history, view their current balance, pay account recipients, perform transfers and third-party payments, purchasing airtime, electricity and data bundles.

2.4 Technician

The technician performs maintenance, runs diagnostics and replenishes the cash reserves. They need access to the ATM system software as well as physical access to the ATM's components, such as cameras, biometrics, screen, keypad and cash safe, to ensure they are functioning properly.

3 Functional Requirements

R1. The system shall allow the user to create an account.
- **R1.1.** The system shall allow the user to create an account at a physical ATM.
- **R1.2.** The system shall allow the user to create an account on their smartphone or tablet device.

R2. The system shall allow the user to sign in and out of their account on their smartphone or tablet device using a single factor authentication.

R3. The system shall allow the user to modify their account details.

R4. The system shall allow the user to delete their account.

R5. The system shall allow the user to make cash withdrawals.

R6. The system shall allow the user to make cash deposits.

R7. The system shall allow the user to make balance inquiries.

R8. The system shall allow the user to interact with ATMs only if they have been two-factor authenticated.

R9. The system shall allow the user to choose which method(s) of authentication they wish to use when interacting with the system.

R9.1. The system shall allow the user to choose between using a PIN or fingerprint as the second factor in the authentication process.

R10. The system shall be online and operational 24/7.

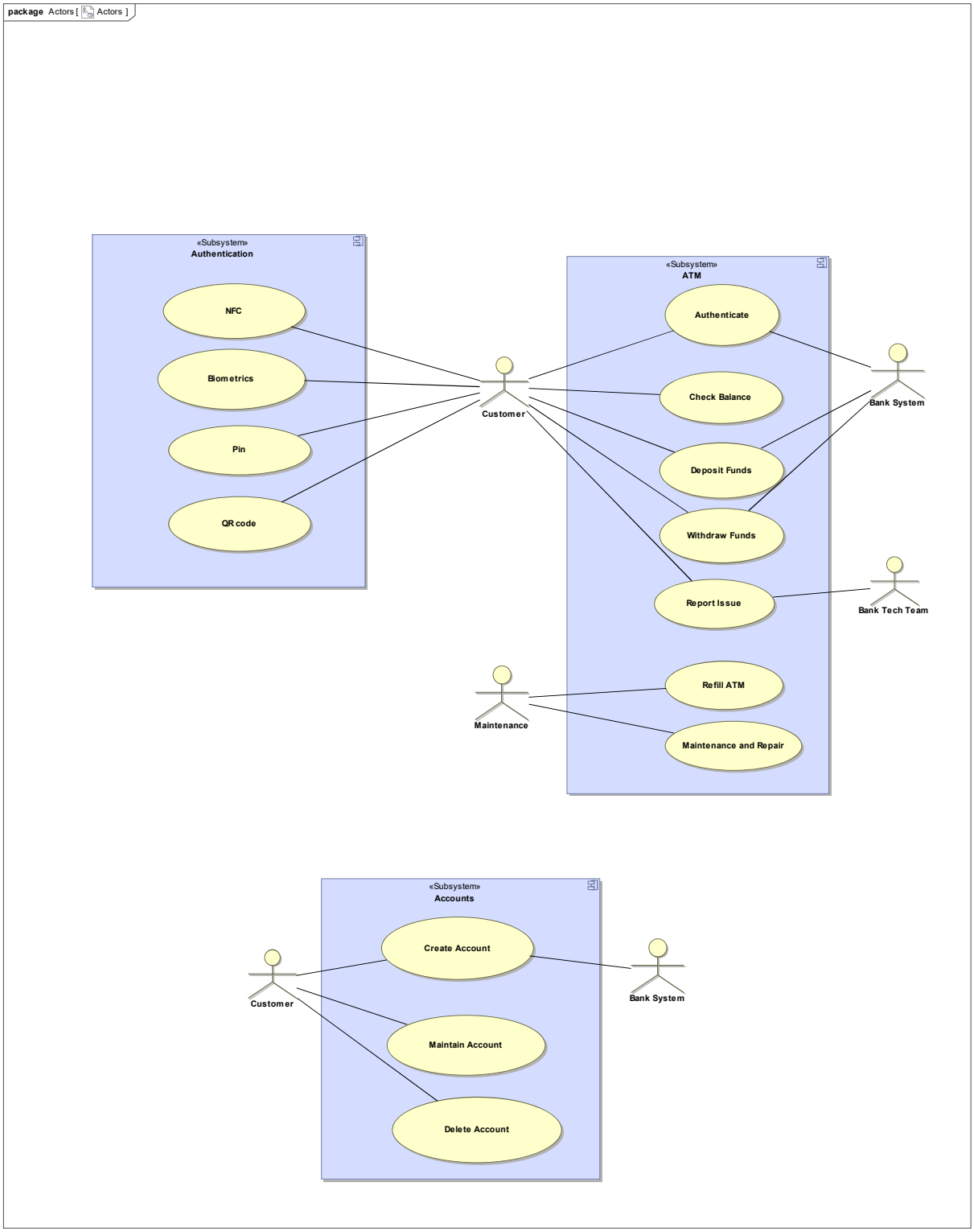
R11. The system shall allow the user to view all ATMs currently active in the system on a map.

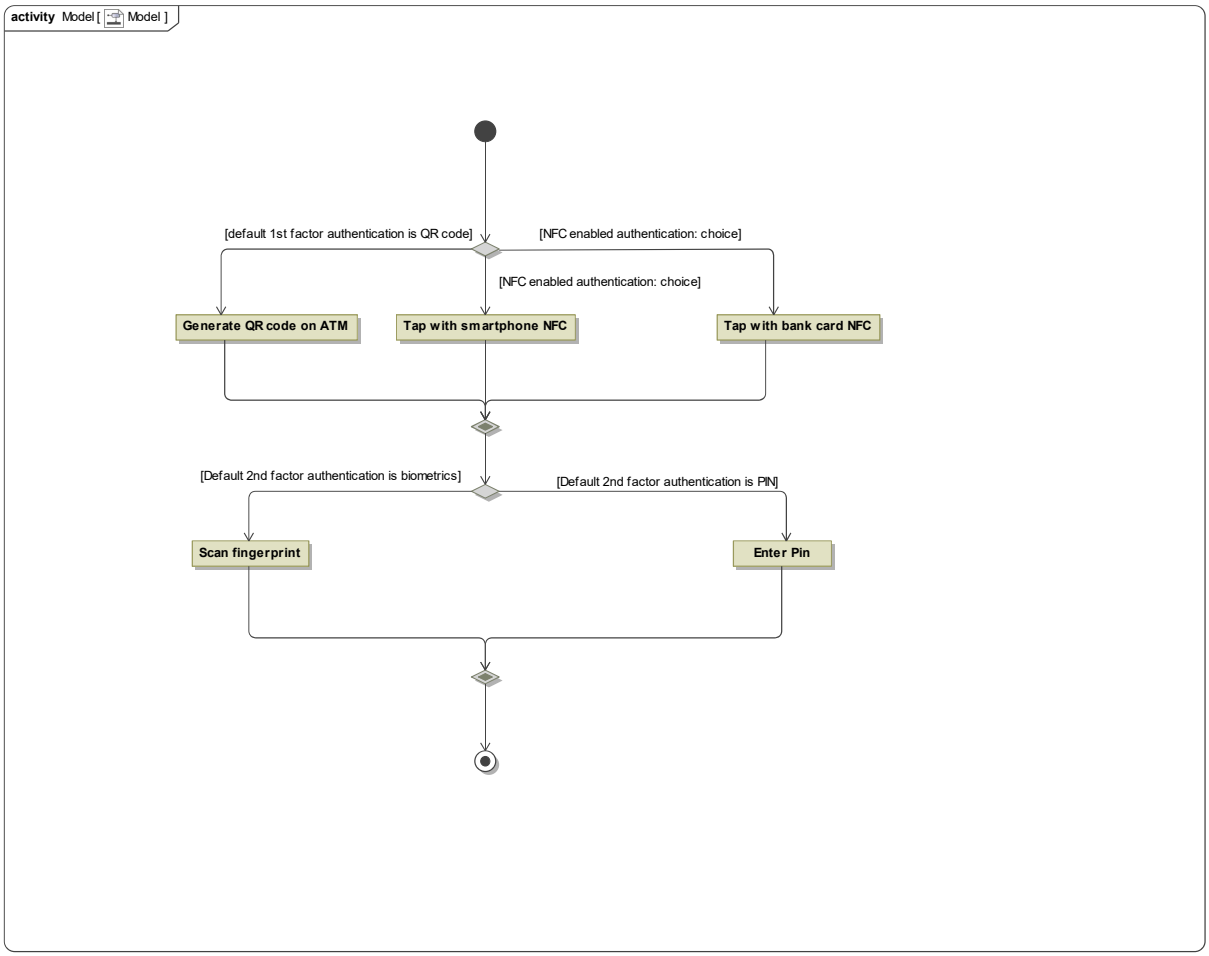
R11.1. The system shall indicate to the user if an ATM does not contain cash, or non-functional due to maintenance or need thereof.

R12. The system shall allow the user to use a session/token[9] based mode of interaction with the physical ATM.

3.1 UML Diagrams

A general use case diagram[16] is presented on the next page. An activity diagram[15] is also provided to demonstrate the flexibility of the authentication process.


package Actors [Actors]
«Subsystem»
Authentication
NFC
Biometrics
Pin
QR code
Customer
«Subsystem»
ATM
Authenticate
Check Balance
Deposit Funds
Withdraw Funds
Report Issue
Refill ATM
Maintenance and Repair
Bank System
Bank Tech Team
Maintenance
«Subsystem»
Accounts
Create Account
Maintain Account
Delete Account
Customer
Bank System


activity Model [Model]
[default 1st factor authentication is QR code]
[NFC enabled authentication: choice]
[NFC enabled authentication: choice]
Generate QR code on ATM
Tap with smartphone NFC
Tap with bank card NFC
[Default 2nd factor authentication is biometrics]
[Default 2nd factor authentication is PIN]
Scan fingerprint
Enter Pin

4 Quality requirements

4.1 Performance

The system is designed to perform mainly, cash deposits, cash withdrawals and statement retrievals. Our design focuses on ensuring that each function runs in a timely fashion.

This will be achieved by ensuring that our system is designed to:

- Process a high number of requests and responses at any given time.
- Handle request of all sizes.
- Service a request that doesn't need reporting in under 2 second.
- Send request to the server from the client in under 1 second.
- Send a respond to the client from the server in under 1 second.
- Service chatbot requests in under 5 seconds.
- Send chatbot responds in under 2 seconds.

This can be achieved by ensuring:

- We use precompiled SQL[7] statements.
- By using cached responses that can be easily accessed.

4.2 Reliability

We aim in ensuring our system is reliable, so users are confident in our product and feel that our system is designed for the best interest of our users.

Our system will be highly reliable because:

- It can be accessed and used from any location.
- Users do not need data bundles to be able to use the services.
- The system will send crash reports to the client if any crashes occur.
- If the server crashes, users will be notified, and given an estimated downtime.

4.3 Security

Our system aims to ensure that user information is protected, through authentication, authorization, and data security. Due to the nature of the banking and investment industry, extra attention will be put into the safety, security, ethical and legal treatment of the customer's information. Two important concepts that will be relevant here are KYC[4] and FICA.[11]

4.3.1 Authentication

Our System will first identify the user. This will be achieved using 2FA[6] (Two Factor Authentication), namely:

- NFC – By means of a smartphone or an NFC ATM card, issued by the bank.
- And a Password – Generated by the user.
- Or Biometrics – This will be optional, based on user preference.

4.3.2 Authorization

Our system will only allow access to users who have been authenticated. Once a user has entered their information correctly, and our system has identified the user, the user will be given access to their requested services.

These services can either be for the:

- Customer – User who makes cash withdrawals, deposits and statement retrievals.
- Admin – User who works for the bank, eg. The Technician

4.3.3 Data Security

To ensure that our user's data is protected, our system will encrypt and salt all confidential user information such as:

- passwords
- biometrics
- user id's.

Also, to protect user information in the case that a device is lost or stolen, our system will use token-based authentication, which only store tokens on user devices, that way information can be cancelled if needed.

4.4 Scalability

> *"Over 1.5 million active devices currently use the FNB Banking App"*
>
> *- Sahil Mungar*

Our system aims to handle and scale all services needed by users at any given time. Our system should be able to allow roughly:

- 1500000 / 24 = 62500 concurrent users per hour.
- 62500/60 = 1042 concurrent users per second.

Given that all users use our system in a day.

4.5 Flexibility

Our system aims to be flexible and be able to adjust to newer technologies and systems. We aim to ensure that our system:

- Is feasible to technological upgrades and updates.
- Database module is feasible to data expansions.
- Authentication module is feasible to authentication protocol upgrades.
- User management module is feasible to modifications and updates.

All this will be achieved by ensuring that all modules run independently and that no modules are coupled with one another. That way upgrades and changes can be made to specific modules without interfering with other modules of the system.

Having a flexible system also means that maintenance is easier and less expensive.

4.6 Auditability

Our system database will be highly monitored and protected, with read-only permissions, so that all activity on the system is recorded and cannot be manipulated. It will be able to keep track of:

- User who logged in.
- Time that user logged in.
- Changes made by the user.
- Activity that user performed.
- Time when user logged out.

4.7 Usability

Our system will be easy to use, this will be achieved through the use of a user-centred navigation design. The aim is to ensure that our system is user friendly, and that all users can use the application, without needing any guidance or extensive computer skills. Our system will also incorporate an intelligent chatbot, which will offer help to users who may have any questions.

5 Trace-ability matrix

Requirement	Priority	UC1	UC2	UC3	UC4	UC5	UC6	UC7	UC8	UC9	UC10	UC11	UC12	UC13	UC14
R1	1	x			x										
R1.1	1	x	x		x										
R1.2	2	x	x		x										
R2	3		x	x	x	x									
R3	1		x	x	x	x									
R4	1				x										
R5	5				x		x	x		x					
R6	5				x		x	x	x	x					
R7	5				x	x									
R8	5				x	x	x				x	x	x	x	x
R9	4				x	x					x	x	x	x	x
R9.1	4				x	x						x	x	x	x
R10	5	x	x			x					x				
R11	3				x				x						
R11.1	5			x	x		x	x	x	x					x
R12	5				x							x	x	x	x
UC Priority		1	2	3	1	5	5	5	5	4	4	5	3	1	5

References

[1] Duncan Alfreds. *Growth in SA mobile banking use - FNB*. 2015. URL: https://www.fin24.com/Tech/News/Growth-in-SA-mobile-banking-use-FNB-20151022 (visited on 02/21/2019).

[2] Liane Cassavoy. *What Is a QR Code?* 2018. URL: https://www.lifewire.com/the-definition-of-qr-codes-578656 (visited on 02/21/2019).

[3] Mike Chapple. *What Is a Database?* 2019. URL: https://www.lifewire.com/what-is-a-database-1019737 (visited on 02/19/2019).

[4] James Chen. *Know Your Client - KYC*. 2018. URL: https://www.investopedia.com/terms/k/knowyourclient.asp (visited on 02/21/2019).

[5] James Chen. *Stakeholder*. 2018. URL: https://www.investopedia.com/terms/s/stakeholder.asp (visited on 02/16/2019).

[6] Jason Cipriani. *Two-factor authentication: What you need to know (FAQ)*. 2015. URL: https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/ (visited on 02/21/2019).

[7] The Editors of Encyclopaedia Britannica. *SQL*. URL: https://www.britannica.com/technology/SQL (visited on 02/21/2019).

[8] Computer Hope. *PIN*. 2017. URL: https://www.computerhope.com/jargon/p/pin.htm (visited on 02/21/2019).

[9] Sherry Hsu. *Session vs Token Based Authentication*. 2018. URL: https://medium.com/@sherryhsu/session-vs-token-based-authentication-11a6c5ac45e4 (visited on 02/21/2019).

[10] Julia Kagan. *Automated Teller Machine - ATM*. 2018. URL: https://www.investopedia.com/terms/a/atm.asp (visited on 02/18/2019).

[11] Julia Kagan. *Federal Insurance Contributions Act (FICA)*. 2018. URL: https://www.investopedia.com/terms/f/fica.asp (visited on 02/21/2019).

[12] Blake Morgan. *What Is A Chatbot, And Why Is It Important For Customer Experience?* 2017. URL: https://www.forbes.com/sites/blakemorgan/2017/03/09/what-is-a-chatbot-and-why-is-it-important-for-customer-experience/#2f14d6747188 (visited on 02/21/2019).

[13] Robert Triggs. *What is NFC & how does it work?* 2018. URL: https://www.androidauthority.com/what-is-nfc-270730/ (visited on 02/18/2019).

[14] *What Are Biometrics*. URL: https://findbiometrics.com/what-are-biometrics/ (visited on 02/16/2019).

[15] *What is Activity Diagram?* URL: https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-activity-diagram/ (visited on 02/21/2019).

[16] *What is Use Case Diagram?* URL: https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-use-case-diagram/ (visited on 02/21/2019).

[17] Staff Writer. *South African criminal reveals how they steal your bank card at an ATM*. 2016. URL: https://mybroadband.co.za/news/banking/171377-south-african-criminal-reveals-how-they-steal-your-bank-card-at-an-atm.html (visited on 02/20/2019).