Software Requirement Specification

Janse Van Vuuren, Bryan
u16217498

Bresler, Mathilda Anna
u16313382

Petrou, Alexandros Mendes
u15291792

Opperman, Christiaan Philippus
u17023239

Li, Xiao Jian
u16099860

February 2019

1 Introduction

1.1 Purpose

In the last two decades a great many advances have been made in technology, which affects multiple aspects of the every day lives of the individual. The traditional ATM systems are becoming outdated and impractical and needs to be re-evaluated to keep up with current lifestyle of people. In this document a system will be proposed that integrates the new technology available with the traditional ATM system, resulting in a *next generation* Automatic Teller Machine System. The documentation will provide explanations about the interactions/relationship between the user, banking application and ATM as well as define system limitations and restrictions which should clarify what the system will be able to accomplish and what constraints the system will have.

1.2 Scope

We extended the traditional scope of the ATM(Automatic Teller Machine) System to include a mobile application that will interact with the ATM and provide additional functionality that overlaps with the traditional ATM system. The *next generation* Automatic Teller Machine System describes a system that provides the traditional functionality that users are familiar with, and new options and functions that will improve the system as a whole. Users will be able to set the amount of money that they would like to withdraw at the ATM from their mobile application, as well as being able to choose the bill distribution they would prefer. Users using the FNB application will also be able to identify the closest ATM in their vicinity, or another specified location, with the sufficient amount of specified cash notes available, so that when they arrive at the ATM they can pick up the money simply by scanning their phone NFC chips to the ATM and verifying their bio-metrics or pin-number. This option will not only minimize the lines at ATM's (due to shorter amount of time waiting in line), but will also decrease the amount of ATM's that will need to be installed since they will be easier for users to locate. The system also has a feature that allows users to set up a 'withdrawal profile' - where they use the application to choose a withdrawal amount, time-frame, and/or area. Once this is set up the user can access ATM's that satisfy the requirement using only their bio-metrics and pin. This allows for users to travel without the fear of losing their phones/cards, and is especially useful in the case of shared accounts. Performance of the system as a whole will greatly be increased as the time it takes for people to withdraw or pay for products will be much quicker than traditional methods. A lot of processing strain will be taken off of the individual ATM's because the mobile device will be doing some of the processing through the application. The whole process of creating transactions will be more familiar to the users as mobile devices are very common amongst most people. The familiarity of the smart phone will help people adjust to the changes of the new system quicker as well as decrease the throughput at the individual ATM's and rather increase throughput through the users mobile device. Using the application on mobile device will also allow updates to be more easily done as the application will be updated either through the Google app store or iOS store.

1.3 Definitions, Acronyms, and Abbreviations

Term	**Definition**
Account Holder	A user who will have an account with FNB
Application	Refers to the *next generation0* Automatic Teller Machine System interface that is accessed through a mobile device
ATM	Automatic Teller Machine
Automatic Teller Machine	A machine which allows for users to interact with banking interface to accomplish simple goals such as withdraws, balance checking and mini-statement
Balance	The current amount of money a user has in their accounts
Bio-metric	Refers to the fingerprint of the user
Card	Refers to a credit card
Cron	A system command that is issues at a specific time for a job execution
FNB	First National Bank
FNB Bank Employee	a system administrator with permission to capture data on new users just padding some text here to test if this will make a new paragraph
Pin	Personal identification number
KYC	Know Your Customer
Mini-statement	A list of transactions that has taken place from a set date to another set date
User	Someone who will interact with the application or ATM
Withdraw	The action of receiving cash from an ATM

1.4 References

Department of CSE. (2015). Software Requirements Specification ATM. In: Department of CSE Software Engineering and Project Management Lab Manual. Indore: Department of CSE. 1-17.

En.wiktionary.org. (2019). monitorability - Wiktionary. [online] Available at: https://en.wiktionary.org/wiki/monitorability [Accessed 16 Feb. 2019].

En.wikipedia.org. (2019). Scalability testing. [online] Available at: https://en.wikipedia.org/wiki/Scalability$_testing[Accessed16Feb.2019]$.

$Gordonedu.2019.Gordonedu.[Online].[14February2019].Availablefrom:http://www.math-cs.gordon.edu/courses/cs211/ATMExample/UseCases.html.$

Peach Payments Support. (2019). Compliance with The Protection of Personal Information Act (POPI Act).
[online] Available at: https://support.peachpayments.com/hc/en-us/articles

/360015955812-Compliance-with-The-Protection-of-Personal-Information-Act-POPI-Act- [Accessed 15 Feb. 2019].

Pimentel, M. (2019). KYC process steps: Humans and Automation and Why Both are Needed. [online] encompasscorporation.com. Available at: https://www.encompasscorporation.com/blog/kyc-process-steps-automate/ [Accessed 15 Feb. 2019].

Training, S., Level, I., Manager, I., Tutorial, A., Tests, I., Us, C., Policy, P., Use, T. and Us, A. (2019). What is Maintainability testing in software?. [online] Tryqa.com. Available at: http://tryqa.com/what-is-maintainability-testing-in-software/ [Accessed 16 Feb. 2019].

1.5 Overview

- **Section 1:** Describes the main purpose of the system, it's scope, and relevant information to interpret the rest of the document.
- **Section 2:** Specifies the different users that will make use of the system and it's sub-systems, and their expected adaptability to the new system.
- **Section 3:** Specifies the components and the interactions among them that are required for the system to be functional.
- **Section 4:** Outlines the Quality requirements that the system needs to fulfill, and a means of testing whether the system adheres to these requirements.
- **Section 5:** Shows the requirements of the system, and whether they are met by the Use-cases.

2 User characteristics

Client: A regular user of the ATM that can range from little to no experience to being an advanced user. The ATM will have a user friendly interface with minimal easy to follow instruction's that will guide the user from logging into their account to using every function the ATM has to offer.

Employee: This user works for the Bank and needs to be able to access the system and be able to perform the basic CRUD (Create, Read, Update, Delete) functions on the user-database.

Back-end: This user is the administrator of the ATM system. This user will know exactly how the ATM operates and will be responsible for maintaining, updating, and monitoring the system. The ATM's administrator's interface will allow for the user to perform error handling, as well as see all the logs and other relevant information.

3 Functional requirements

3.1 Application verification - *UC1*

This is necessary to verify that the account set up on the device belongs to the owner of that account, this is for security reasons. The two Actors in this case is the Bank employee, and the account holder(who will be the user in this case). The user first needs to have the application installed on their mobile device. To link the users account with the application on the specific device (NFC chip) the Bank employee opens the users account, then captures the user's identifying information(pin and bio-metrics). If the user is successfully authorized they receive a message from the Bank with a One-time-pin that allows them to enter and take ownership of the application on their device.

3.2 Balance inquiry

3.2.1 Balance inquiry at ATM - *UC2*

The Actors involved are the FNB server, the ATM, and the ATM user. The ATM displays instructions for the user to identify themselves. The user can tap their card or mobile device's NFC chip against the ATM's NFC reader. Alternatively the user can use bio-metric information by scanning their fingerprint on the bio-metric reader. The ATM then sends the captured data to the FNB server, where the user's account information is retrieved. The server then responds to the ATM requesting user data for authentication. In case of card or mobile device identification the user is prompted to provide their pin and their fingerprint. In case of bio-metric identification the user is prompted for their pin only. This data is then transmitted to the server where it is checked against the user's information. The server responds with a success or failure code. If the ATM receives a success code the user can choose to view their balance, this is then displayed on the screen. If a failure code is received an appropriate error message is displayed to the user. The user is then logged out, and the user session is terminated.

3.2.2 Balance inquiry using mobile application - *UC3*

The Actors involved are the user, the mobile banking application, and the bank server. The user logs into their mobile application using their bio-metric information and their pin. The login process consists of the application sending the data provided by the user to the bank server, where it is used to authenticate the user. If the authentication is successful the server sends a success code to the mobile application, the user can then select the view balance option on the application. The application sends the request to the server, which selects the relevant information from the user's profile, and sends the information to the mobile application, where it is displayed to the user. If the authentication process failed, the server send a failure code to the application, and the appropriate error message is displayed to the user. The user is then logged out, and the user session is terminated.

3.3 Requesting mini-statements

3.3.1 Requesting mini-statement at ATM - *UC4*

The Actors involved are the FNB server, the ATM, and the ATM user. The ATM displays instructions for the user to identify themselves. The user can tap their card or mobile device's NFC chip against the ATM's NFC reader. Alternatively the user can use bio-metric information by scanning their fingerprint on the bio-metric reader. The ATM then sends the captured data to the FNB server, where the user's account information is retrieved. The server then responds to the ATM requesting user data for authentication. In case of card or mobile device identification the user is prompted to provide their pin and their fingerprint. In case of bio-metric identification the user is prompted for their pin only. This data is then transmitted to the server where it is checked against the user's information. The server responds with a success or failure code. If the ATM receives a success code the user can choose to receive a mini-statement, by either displaying on the screen or printed on a slip the user can retrieve from the ATM. If a failure code is received an appropriate error message is displayed to the user.The user is then logged out, and the user session is terminated.

3.3.2 Requesting mini-statement using mobile application - *UC5*

The Actors involved are the user, the mobile banking application, and the bank server. The user logs into their mobile application using their bio-metric information and their pin. The login process consists of the application sending the data provided by the user to the bank server, where it is used to authenticate the user. If the authentication is successful the server sends a success code to the mobile application, the user can then select the view mini-statement option on the application, the user can provide additional information which includes date range, transaction type, specific beneficiaries, amongst other options. The application sends this request to the server, which selects the relevant information from the user's profile, and sends the information to the mobile application, where it is displayed to the user. If the authentication process failed, the server send a failure code to the application, and the appropriate error message is displayed to the user. The user is then logged out, and the user session is terminated.

3.4 Money Withdrawal

3.4.1 Money withdrawal with card- *UC6*

The three actors involved are the FNB server, the ATM, and the ATM user. The ATM displays instructions for the user to identify themselves, and in this case the user taps their card against the NFC reader, the ATM then prompts the user to scan their fingerprint or enter their pin. The ATM then sends this information to the server where the transmitted data is compared to the saved data in the user profile (which is identified using the information on the card). If the information matches, the server responds to the ATM with a success code. The user can then selects the option to draw money from the ATM. The ATM sends this request to the server, the server attempts to process the request.If the request cannot be processed or the information is invalid an invalid code is sent to the ATM. The user then receives their cash or is displayed an appropriate error message.The user is then logged out, and the user session is terminated.

3.4.2 Money withdrawal with application- *UC7*

The four actors involved are the FNB server, the ATM, the user and the FNB application. The application provides an interface for the user to interact with. The user can now select from the application the amount of money they would like to withdraw and the application calls the servers to create a temporary priority withdraw log of the transaction and stores it will also generating a set of ATMs that are located close to the current user's location that meets the requirement of containing the sufficient amount of cash notes. The application will take this information and display it to the user. The user can now approach the preferred ATM of choice and interact with the ATM. The interaction will consist of the user tapping their phone to the ATM's NFC scanner, this will prompt the ATM to send a request to the FNB server to identify if there is currently a priority withdraw transaction log available for the current user; if not refer to subsection:" Application verification ***- UC1*** " else if a priority withdraw transaction log exist then the server will send a notification to the ATM asking for bio-metric verification, once confirmed the ATM will give the user the requested amount as well as update the priority withdraw transaction log to completed. The user is then logged out, and the user session is terminated.

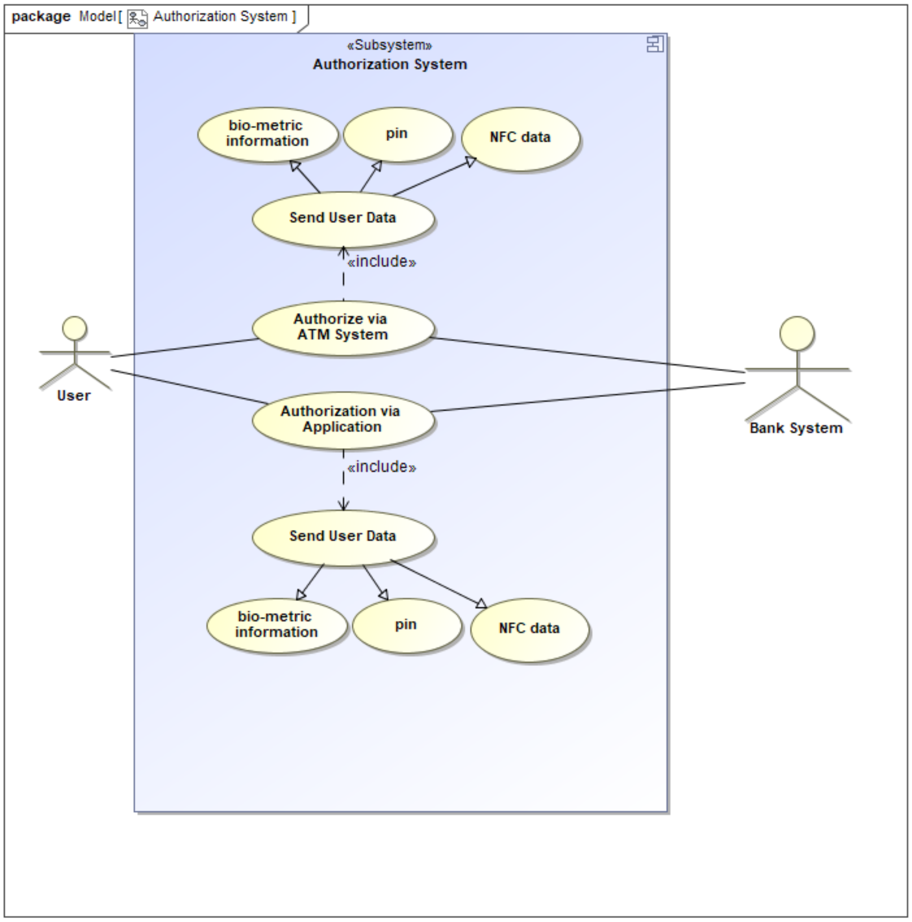
3.4.3 Money withdrawal/payment using mobile device's NFC chip - *UC8*

The actors involved are the user, the FNB mobile application, the vendor or ATM involved, and the FNB servers. The user either selects to withdraw money from the ATM, or the vendor elicits the required amount. The user then taps their mobile device against the NFC reader, the ATM/vendor then send the request to the server. The server locates the user's profile and send a notification to the user's mobile application that then proceeds to prompt the user to approve the request by means of bio-metric information as well as their pin. The application then sends this information back to the server, where it undergoes verification. If it is successful the transaction is processed and the relevant logs are updated as well as the users account. If the option was to withdraw money the user receives their cash, if it was vendor payment the money is transferred to the relevant account.The user is then logged out, and the user session is terminated.

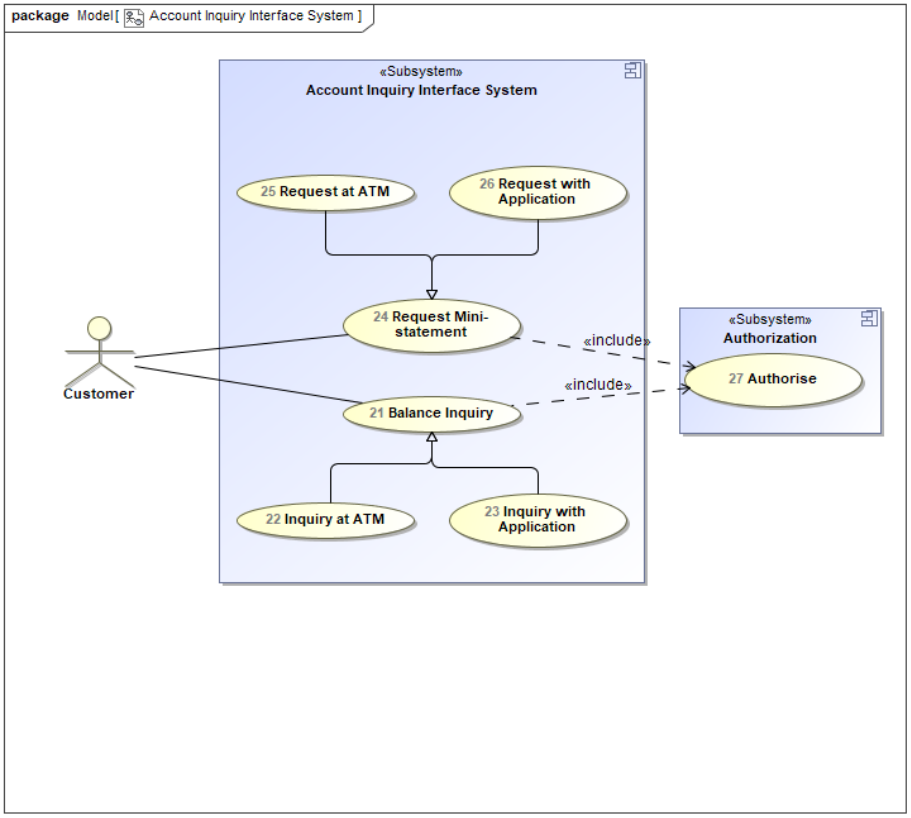
3.5 ATM and Bank interaction- *UC9*

This use case is outside the scope of the project, however it is needed to satisfy some of the system requirements. The actors involved are the ATM, the bank system, and the customers. Actions that can be performed include the Bank being able to interact with the bank's servers, as well as the ATM interacting with the server, and the customer with the customer.

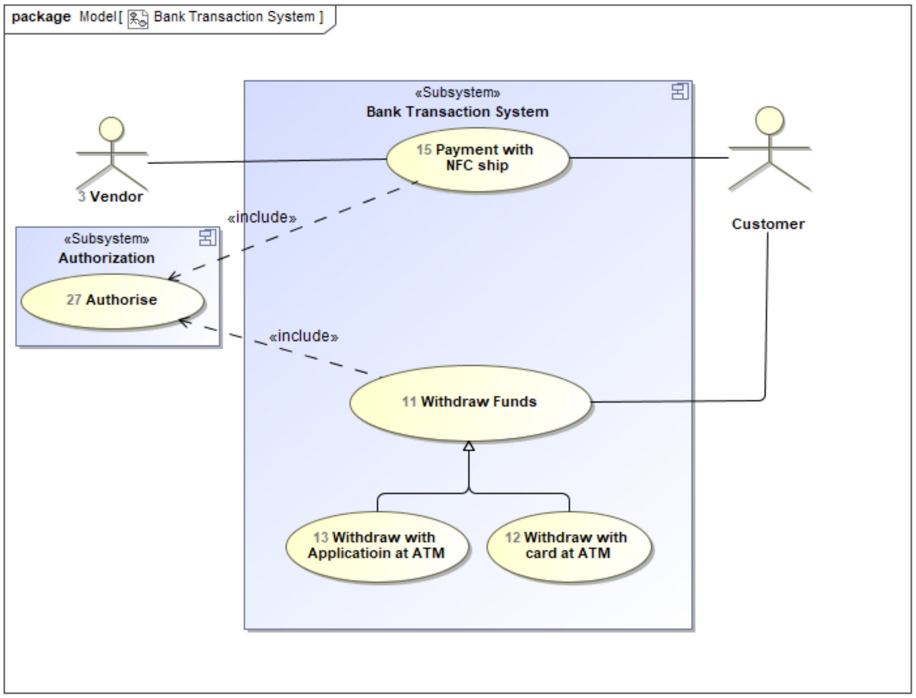
3.6 Authentication System- *S1*



3.7 Account Interface System- *S2*


package Model [Account Inquiry Interface System]
«Subsystem»
Account Inquiry Interface System
25 Request at ATM
26 Request with Application
24 Request Mini-statement
21 Balance Inquiry
22 Inquiry at ATM
23 Inquiry with Application
Customer
«include»
«include»
«Subsystem»
Authorization
27 Authorise

3.8 Transaction System- *S3*



4 Quality requirements- *S4*

4.1 Performance

The system as a whole must be able to perform at high speed and great volumes. There are various factors that need to be kept in mind when testing the performance: The type of point of sale, which could be the physical ATM, the banking app, or private vendors. The geographical location and it's network connection. And the physical conditions that the system will function under. The most important factor to test is the handling of large transaction volumes, the validation of the data transferred by the system, and the response time the user experiences. To test the performance of the ATM system a program with random but valid data can continuously create transactions on the ATM and emulate different ATM's. The same can be done with the mobile application.FNB Tap and pin system currently saves the user 20 seconds of a transaction.This new system will save the same amount of time,if not more depending on if user selects amount through the application at home. The speed to create a transaction will be improved roughly by 20 percent.

4.2 Reliability

The system needs to be as reliable as the current ATM system if not more reliable. The system needs to be reliable when a user uses their mobile device to approve a transaction.A reliable system will provide correct data at correct times. To test reliability of the ATM system users must create transactions one after the other and at the same time.The same tests can be done using mobile version of the application. With transactions being created we can see the reliability of the NFC readers as well as bio-metrics on approval. The system reliability can also be seen with response time to users and notification times on mobile device.

4.3 Security

The system must be highly secured and encrypted. User data must be encrypted preventing FNB from viewing user sensitive information. Transactions must be secure from thieves thus the ability of using bio-metrics instead of pins. Data needs to be encrypted so that even if data is somehow captured from outside parties it can not be read or interpreted. To test the security of the system outside parties(Trained teams part of testing security) could try and breach the system either through the app or other means. Feedback from these teams would help identify security issues. Other ways of testing security would be to have users swap devices and try and create transactions off those devices. Security features need to be strong enough to comply with the POPI act, meaning that the customer's personal information will be kept secure, and that the organization will be aware of who has access to what information. It is also important that the employees of the business is made aware of the policies that they must comply with to prevent them from unknowingly breaching the companies security(Peach Payments Support, 2019). Creating transactions will now be on average 50 percent safer as two factor authentication is required and criminals will be less likely to steal your data as biometrics is also needed.

4.4 Maintainability

The system maintenance can falls under two distinct categories, that being hardware maintenance and software maintenance. These system maintenance are required to ensure minimal system malfunctions occurs and that systems are always up to date with the latest functionality.

Malfunctions which prevent proper functionality at ATMs or cash vendors, such as bio-metric scanners unable to detect or identify bio-metrics or NFC readers unable to read users' NFC chip located on their phones, will fall under the category of hardware maintenance.

Testing for hardware malfunctions can be done through either the use of a cron which should run at the beginning of each day every ATMs, this cron can be used to provide a system check logging and identify, in small local cache memory, if each sub-system of the ATM is functional. If the system check identifies a fault it can then send a log to the FNB servers requesting for immediate repairs and also classifying itself as non-functional to the app. Another means of testing for hardware malfunctions can be that of logging the length of each transaction occurring at the current ATM to detect for anomalies.

The software maintenance will be done through either patches or updates depending on the scale in which the current version of the interface found on an ATM, cash vendor or phone application is differs from the latest version of the interface. The ATMs and cash vendors should be able to automatically download and install any patches/updates in order to maintain version consistency with the main system.

4.5 Scalability

The scalability will depend on FNB's servers. To test the scalability of the new system increment loads could be done where one would add a group of new users and see if it affects performance of the system and adjust accordingly. Because it is difficult to predict the number of users over the course of the applications life cycle scalability would need to be tested through out the applications life cycle. KYC processes can slow down the growth of an organization if it is manually handled. However thanks to improvements in technology many of the steps in the process can be automated. It is therefore important to implement a sufficient Intelligent Process Automation system to make bio-metric systems feasible on large scales(Pimentel, 2019).

4.6 Cost

The bulk of the initial expenses will be to cover for the cost of integrating the *next generation* Automatic Teller Machine System and with that installing biometric scanners. This cost will be less than market price, because FNB will buy it in bulk. There will be cost additional costs concerning the app and severs, but this will be minimal because FNB already has the infra-structure in place. Costs could increment as more users and thus more servers will be needed to support the system and have it performing at its peak. Costing of the system would need to include the upgrades of ATM's,Advertising the new system, and all maintenance costs of the system.

4.7 Usability

Since people are already using the app, the new addition to this app will function in a similar manner, which will make it intuitive to use. The simple design and functionality will also add to it being user friendly. (We can add a help function to improve usability.) Testing usability would require prototyping and lots of user demo's which will monitor user thoughts on application as well as if they notice increased ease of use over traditional system.FNB application volume climbed by 65 percent in 2018. Thus there are more users becoming familiar with the application side of banking, making usability easier to test and receive feedback. With ease of using application and current generation mostly all being technologically inclined FNB can expect a climb of 30 percent in their application downloads.

4.8 Flexibility

The system will be flexible in the sense it can adapt to future changes. The system will be flexible in the sense that updates can be done remotely and hardware will be sufficient for many years going forward. This would help reduce costs of upgrading the whole system every n years saving FNB a lot of money in the future.

4.9 Monitorability

The new ATM system needs to be able to be monitored constantly to ensure validity,performance and security of the system and its data. To test this, reports on the system can be made on daily basis showing performance, ATM's problems using a mapping system as well as other micro data that can be used to determine health and state of the system. The app would need to be monitored to determine uninstalls and usage of the the new transaction methods.

5 Trace-ability matrix

Requirement	**Priorily**	**S1**	**S2**	**S3**
UC1	1	X		
UC2	1	X	X	
UC3	1	X	X	
UC4	3	X	X	
UC5	3	X	X	
UC6	4	X		X
UC7	2	X		X
UC8	4	X		X
UC9	5	X		
Total		9	4	3