A. MOBILE DEVICE APPLICATION SECURITY ARCHITECTURE

The focus in this section is specifically the security architecture of the *mobile device*.

BACKGROUND
The aim is to authenticate a device and encrypt the data transmitted between the device and a server, particularly to a mobile Application on a mobile phone.

Mobile communications devices such as mobile telephones include a mobile communications network access device, which is typically in the form of a subscriber identity module (SIM). The SIM is an integrated circuit that securely stores a service-subscriber key (IMSI) used to identify a subscriber on a mobile telephony device and allows a device using the SIM access to the mobile network.

The security methodology authenticating the mobile device and encrypting data transmitted between the devices will not use the SIM for authentication and encryption and this will be part of the APP.

SUMMARY OF PROPOSED SECURITY SOLUTION
The method to authenticate a device and encrypt the data transmitted between the device and a server comprises a technique to achieve a sufficient level of mutual authentication between an application on a mobile device (client side) and the legitimate back-end infrastructure (server side). The client authenticates the server using the typical Public/Private Key Infrastructure (PKI), knowing that only the legitimate server has access to its own (the server's) Private Key. The server authenticates the client using a unique identification that is linked to each device. This unique identifier is created during the registration process.

The security solution enables the secure transmission of sensitive information (e.g. financial/payment information: credit and debit card numbers, PINs, etc.) from a mobile device to the associated server and then onwards to a service provider/third party (e.g. financial institution including banks or card associations) without exposing the sensitive information at any point.
For a more detailed document please contact **WIZZIT International.**

WIZZIT International, as a technology driven organization, relies to a great extent on the effective design, implementation and daily use of computer systems. The use of computer systems and their associated applications and services are in part extended and exposed to **WIZZIT** customers.

The use of these computer systems, applications and associated services are governed by:

1. Organizational Procedures, Processes & Policies.
2. Compliance requirements such as POPI, PCI-DSS & FSB-FSA.
3. Governance Principles.
4. Technical system security standards as set forth in the Payment Card Industry Data Security.

WIZZIT MOBILE & ELECTRONIC BANKING PLATFORM

WIZZIT SECURITY RULES MODULE

The **WIZZIT** module has a rules based engine for the organization to apply security rules/measures. These rules contain the following:

PIN AND PASSWORD RULES:

- Minimum & Maximum Lengths
- Numeric / Alphanumeric
- Expiry Date
- Contain Special Characters/ Numeric Characters
- Number of Retries before the Channel is Blocked
- Do Not Allow Certain Values e.g. 1111, 1234

WIZZIT have engaged with an Independent Assessor to assess the cloud system against afore mentioned and to ensure full understanding of associated risks.
It is imperative that WIZZIT conduct such so as to ensure that the financial institution is confident in the solution selected and to:

- Identify compliance deltas within the system that are not in line with the Financial Institutions Standard.
- Identify & quantify risks posed by non-compliant items.
- Provide the Financial Institution with a risk map if required.
- Ensure & prove that a reasonable amount of effort is taken to safeguard confidential data of the Financial Institution.
- Ensure that full or partial safe-harbor is provided by the FSB & associated Banking Providers in case of a data breach.
- Ensure that sufficient measurement metrics exist to gauge & manage compliance & risks items on an ongoing basis (Audits).

The following processes will be followed to ensure security standards are adhered to during the total duration of the cloud:

1. *System Review*
2. *Risk Analysis*
3. *Portal Permissions & Database Security*

The following criteria will be followed for each new implementation:

- Risk assessment report every 6 months based on the current snapshot of the system.
- Comprehensive assessment report before the go live date for all implementations that will provide a full view of security risks, as well as provide recommendations for improvement.

The following details will be documented:

- Security requirements & objectives.
- System or network architecture & infrastructure, such as a network diagram showing how the assets are configured & interconnected.
- Physical assets such as hardware equipment.
- Systems such as operating systems, network management systems.
- Content such as databases & files.
- Application & server information.
- Networking details such as supported protocols & network services offered.
- Access control measures.
- Processes such as business process, computer operation process, network operation process, application operation process, etc.
- Identification & authentication mechanisms.
- Relevant statutory, regulatory & contractual requirements pertaining to minimum security.
- Control requirements.
- Documented or informal policies & guidelines.

The following applications are part of the **WIZZIT** platform and have been broken down into a set number of defined permissions.

- USSD
- APP
- Internet Banking

1. PORTAL PERMISSIONS AND DATABASE SECURITY

PERMISSIONS

The system has been designed around a set number of permissions. These are all pre-configured and are integrated into all the modules of the system. For example a role can be linked to a specific function.

An agent role will be linked to the permission below: USSDAGENT and will then see the USSD Agent Menu. If the role also has access the Mobile Money USSD, then the first USSD menu screen will give the option:

1. Mobile Money
2. Agent

The same as above will apply to the APP.

CONCLUSION

The **WIZZIT** system has been designed to accommodate the banking industries requirements for Security and risk management. We comply with the latest standards and are constantly updating the system with new security features. If there are any additional regional or banking requirements we will accommodate these.

CONTACT US
For more information about the **WIZZIT** Platform for Mobile Banking,
visit www.wizzit-int.com or call +27 11 523 5600 or email info@wizzit-int.com