DHQ/DMI/420/1

BRIEF FOR DMI

THRO' COL IT

OPERATIONALIZATION OF SALAMA MOBILE APPLICATION

COMMENTS

INTRODUCTION

1. The Directorate of Military Intelligence (DMI) has spearheaded the Cyber Command Research, Innovation and Development projects at the MORAN CENTER to develop cyber offensive capabilities and Information Systems for the Kenya Defence Forces (KDF). In the year 2020/21, the DMI had engaged Armour Comms Secure Messenger from an external vendor for secure communication within the directorate. However, purchasing cost, recurring license payments per annum, number of user limitations, inability to modify features as required, maintenance and upgrade costs, challenged the directorate to pursue the cyber capability and skills development IOT enrich KDF's Cyber Capacity with home-grown systems.

2. The research team in turn proposed the Salama Mobile application, that provides end-to-end encrypted messaging, secure file transfer, video and audio calls as well as broadcast news alert within the KDF with features of world-class secure real-time communication to replace the Armour Comms and provide similar functionalities in the WhatsApp, Signal and Telegram Messengers. The App will be available on the iOS App Store and the Android Play Store for ease of secure downloads and updates.

SALAMA MOBILE FEATURES

3. The development phases of the application are at near-complete stages with server system being at 100%, Android version at 90% and iOS version at 80%, with the following features ready to deploy.

a. **Secure Messaging between Users and Groups**: Messages are encrypted at the sending user and only decrypted at the recipient user. Each user and group have own public and private keys.

b. **File Sharing (Images, Videos, Audios and Documents)**: Users can attach file from their devices to share with recipient users with option to encrypt the file. File encryption key is in-built within the application.

c. **Video and Audio Calls**: Users can do one – on – one video or audio calls as well as group video or audio meetings directly on Salama Mobile App.

d. **Channels for Broadcast**: Owing to the KDF requirements in broadcasting news and events through STRATCOM, Salama Mobile has a feature to create channels within the application to allow STRATCOM, DESACCO, DEFCO, DEFMIS, ULINZI SPORTS and any other KDF Institution that need to post important announcements needed to reach KDF Pers within their respective channels.

SECURITY AND ENCRYPTION TECHNOLOGY

4. The Salama Mobile Messaging Platform was built with the security of Comms as its first priority to guarantee the data confidentiality, data integrity and data availability within the KDF.

5. IOT achieve these, all Salama Mobile software codes are developed for and owned by the KDF, encryption technologies are readily available to KDF Cybersecurity experts for verification and further improvements, and all data stored at the server are readily available for the authorised users, hosted securely at DHQ and the MORAN CENTER.

REGISTRATION, VERIFICATION AND AUTHENTICATION OF USERS

6. The Application is an organization-based that requires pre-authorisation of users. There is need for the Development team to have Pers necessary data including service number, phone number, rank, name and appointment for enrolment and identification between users.

7. Upon installation, user will be required to enter a unique organization number, service number and phone number to receive a one-time SMS verification code (OTP) as two-factor authentication mechanism (2FA).

DELIVERY TIMELINES

8. The table below illustrates the project delivery timeline:

Tasks	**Development Stage**	**Pending Features**	**Estimated Completion Date**
App Server	100%		Deployed
Android Version	90%	Channels	30 Sept 2024
IOS Version	80%	Channels, Group Calls Interface	30 Oct 24
Testing & Deployments	Testing within the MORAN CENTER & DHQ CIS	App Store and Play Store	30 OCT 24

STAFF COMMENTS

9. Cyber Command research projects including the Salama Mobile will help the KDF to overcome challenges of relaying on external parties for development and maintenance support hence reducing financial implications.

10. In-house applications guarantee the security of KDF information since administrative access and total control of the applications are in the hands of KDF Pers.

RECOMMENDATIONS

11. The following is recommended:

a. The app be approved for rollout and user testing within selected KDF Pers.

b. The development team be granted access to Pers necessary data for enrolment into the application.

c. The development team to support in-house Apps IOT improve security, stability and functionality.

d. Vulnerability Assessment and Penetration Testing be conducted both internally and externally to test security controls, identify existing weaknesses and simulate cyber-attacks IOT enhance incident prevention and response.

12. Sir, forwarded for your information and further guidance.

Sept 24

T S Hamza
Capt
SOII Applications