APEX CAPITAL RESERVE BANK INC.
Overview of KTT Transmission Framework and Secure Communication Infrastructure

May 1, 2025

I. **Introduction to KTT (Key Tested Telex)**
Key Tested Telex (KTT) is a legacy financial messaging protocol originating from the analog era. Historically employed by international banks to transmit authenticated payment instructions and sensitive communications, KTT operates using a predetermined "key test" formula—where embedded numeric sequences in the message are verified against an agreed-upon cipher to validate authenticity. Though considered an analog format, KTT remains relevant in modern-day financial ecosystems, particularly for institutions or sovereign frameworks operating outside the SWIFT network or seeking a parallel non-digital validation path.

II. **Analog-Digital Integration**
Despite its analog origins, the KTT framework continues to hold operational significance due to its security, point-to-point nature, and independence from global validation infrastructure such as SWIFT. At ACRB, we leverage a hybrid methodology—bridging analog transmission formats with modern encryption standards—to ensure secure communication while maintaining backward compatibility with global receivers still accepting KTT instructions.

III. **ACRB's KTT Transmission Infrastructure**
ACRB does not operate its own analog telex switch directly. Instead, we maintain a fully secured digital interface with a trusted third-party service provider connected to the **Telex By Net** platform. This configuration enables the transmission of KTT messages over a certified analog interface while leveraging digital encryption for integrity and delivery assurance.

What is Telex By Net?

Telex By Net is a secure, analog-compatible transmission network that allows digitally-originated messages to be translated, authenticated, and relayed through traditional telex lines. It serves as a secure bridge between modern financial institutions and traditional telex-compatible receivers—most notably in regions and banks that still rely on legacy systems. Telex By Net is accredited for high-integrity analog communications and is utilized globally in scenarios where SWIFT access is unavailable or undesired.

IV. **ACRB's KTT Workflow**

1. **Message Origination:**
   ACRB uses a secured email interface to initiate KTT message workflows. Each message is composed following the 2022 IOS structured KTT format, including key-tested numerical identifiers used for verification by the receiving institution.

2. **Secure Transmission to 3rd Party:**
   Upon composition, the email body containing the KTT instruction is transmitted via a secure, TLS-encrypted channel to our designated 3rd-party transmission handler.

3. **Message Encryption and Packaging:**
   The third-party system encrypts the content, wraps the message in compliance with Telex By Net encoding requirements, and prepares it for analog relay.

4. **Analog Dispatch via Telex By Net:**
   The encrypted message is routed through Telex By Net to the designated **Telex Number** associated with the recipient institution's KTT terminal.

5. **Delivery and Receipt Confirmation:**
   Upon successful receipt, the recipient's KTT terminal confirms acceptance. A bi-directional report is generated and returned to ACRB's third-party provider, confirming delivery and including the "Sent Message" receipt.

6. **Audit Trail and Compliance:**
   ACRB retains all message logs, key-test confirmations, and receipts within its compliance audit system for regulatory and forensic purposes.

V. **Summary**

The ACRB KTT protocol represents a secure, compliant, and verifiable alternative to digital interbank messaging platforms. By bridging analog integrity with digital delivery and encryption, ACRB continues to support clients and partners requiring secure communication through legacy infrastructure. Our trusted integration with Telex By Net ensures timely and authenticated message delivery, while maintaining strict adherence to regulatory standards and message auditability.