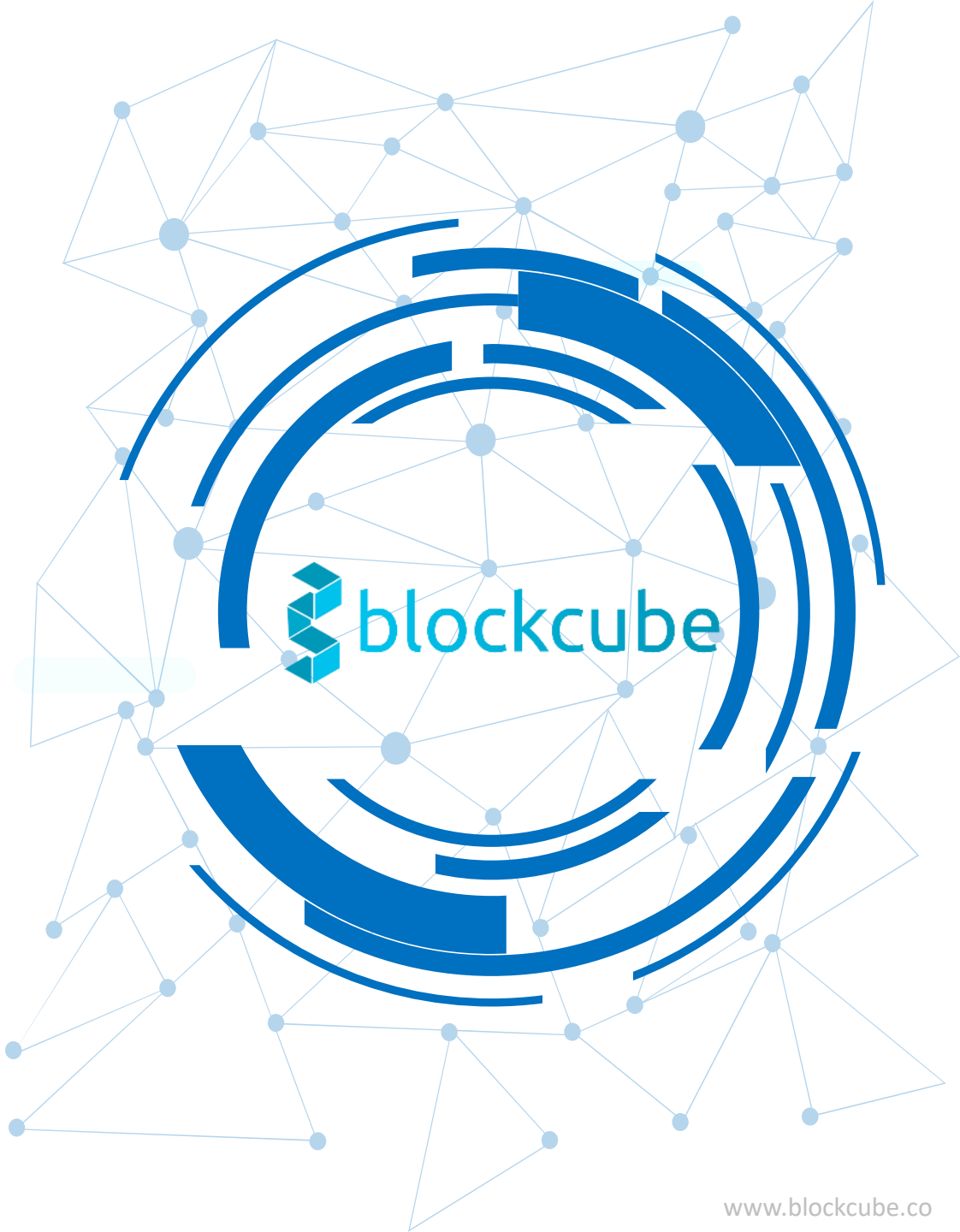
Tamper Proof SMS - Application

Application for Secure SMS Application

Brought to you by Blockcube Technologies.
Blockcube is a Blockchain Consulting, Research & Development Co.



Tamper Proof SMS - Application

Purpose

To achieve more secure SMS delivery to the customers using Encryption and Blockchain technology. Message initiation with two layer encryption, before it reaches to customer.

Scope

The solution will require all participating nodes to be integrated with our application. The Application will ensure seamless and secure collaboration between all the stake holders while maintaining records of the entire SMS flow on Blockchain.

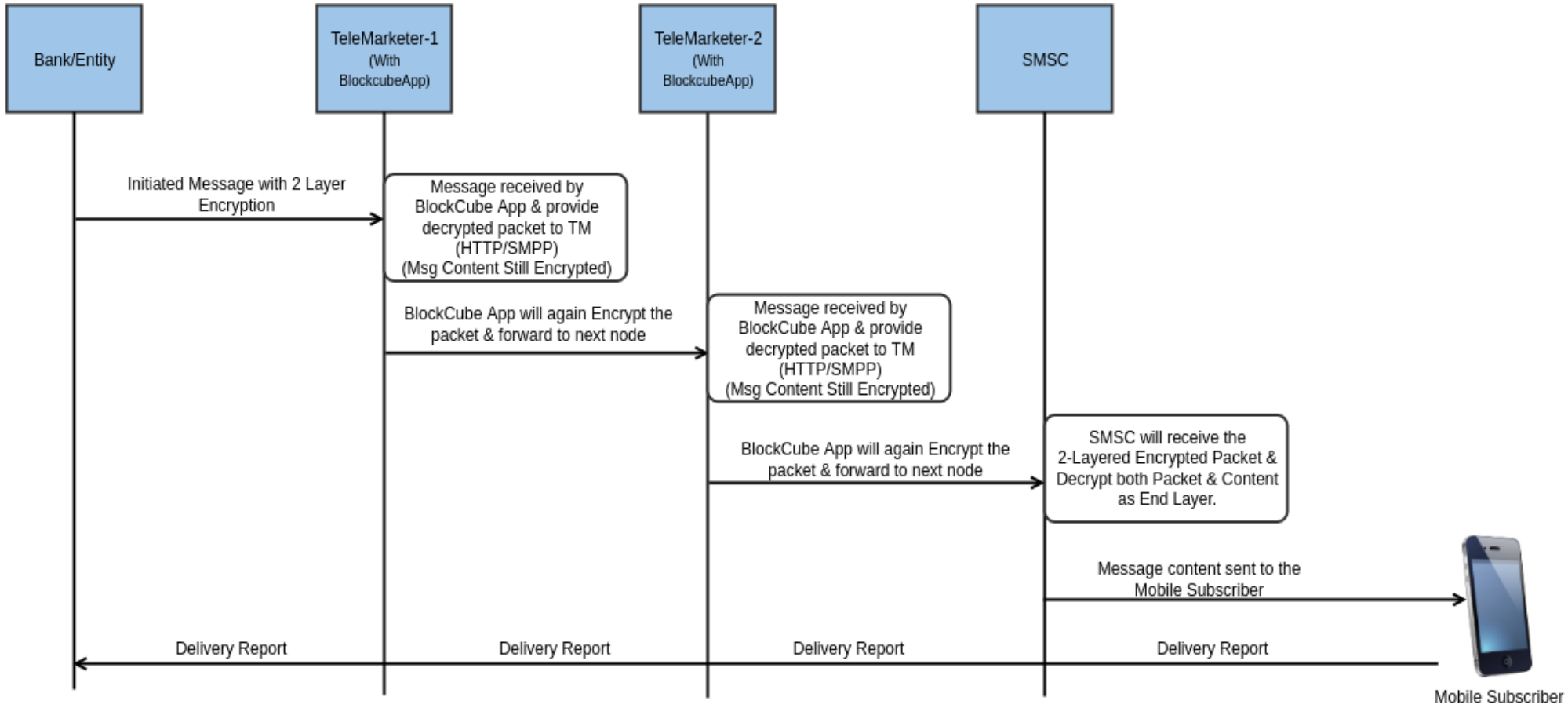
Tamper Proof SMS - Application

Unique Features of Our Application

- Two layer Encryption will be there (Packet & Message Encryption).
- Our application should be deployed on particular node to decode the message.
- Only relevant details will be decoded at nodes(content will remain encrypted).
- TPS will not get effected during processing.
- Tamper proof solution- If tamper attempt, alarm /alert will be generated. Primary entity can block that IP and message.
- Route tracking of IP will be there.
- Data will be stored in blockchain. Primary entity can also check the logs.
- No need to change the current system configuration at any node.
- Easy to integrate, configure and operate.

Tamper Proof SMS - Application

Application Process Flow



Prerequisites - All the SMS transit nodes should have Blockcube's Application. Blockcube's Application supports both Linux & Windows Machines

Tamper Proof SMS - Application

Process Flow - Description

- A Blockcube Application will be installed at Bank's/Entity's Premises & as soon as Bank or Primary Entity will generate the SMS towards assigned destination, 2 Layer Encryption will be done - Complete Packet Encryption (SMPP/HTTP Packets) & Message Content Encryption.

- When Encrypted Packet reaches to Telemarketer/Aggregator's Node, first level of Decryption will take place to provide relevant info to Telemarketer/Aggregator i.e. Header, MSISDN, Source Etc although SMS Content will remain Encrypted & unreadable. This can be repeated to multiple nodes before reaching the End SMSC.

- Once the packet reaches to end SMSC, Blockcube Application will process both layers of Decryption, sends the message to the end user & records the complete message flow to database & blockchain which will be readily available to Bank/Primary Entity to enable traceability.