Secure Digital Banking & Financial Inclusion for 1.7 billion unserved / underserved mobile phone users

Emerging markets in Indian Subcontinent, Africa & S E Asia

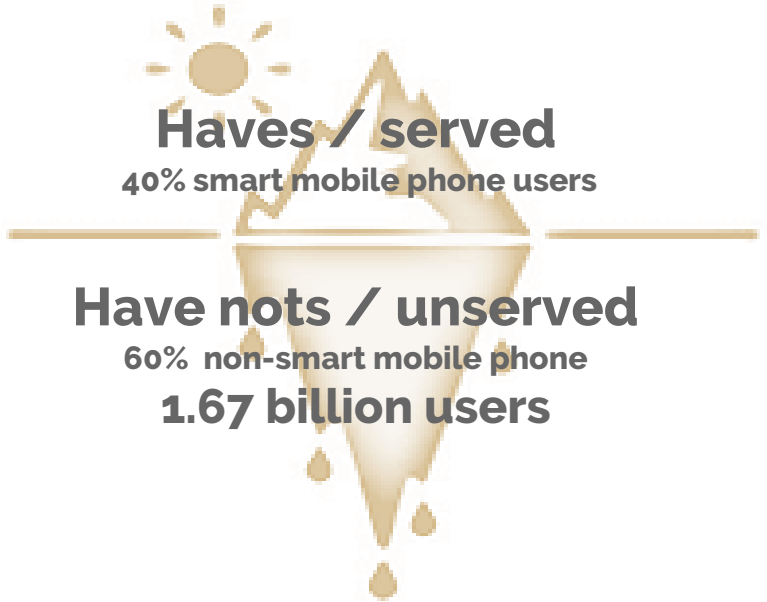
Innovative | Disruptive | Differentiated

Mojaloop & NextGen Objectives Perfectly Aligned

The ***Mojaloop mission*** is to increase financial inclusion by empowering organizations creating interoperable payments systems to enable digital financial services for all

NextGen enables a ***"Secure Bridge"*** for these services with a ready to go, configurable, easy to use and on any mobile device for service providers and the end customer

Financial Inclusion For The Masses



Africa | Asia | South America

The challenge / the need :

- Low end mobile users unserved
- Faces major hardships and costs to handle banking & payments
- Looking for a secure / trusted / simple multi language menu
- Device / network independent
- Multi service offering
- User education on trust and usability

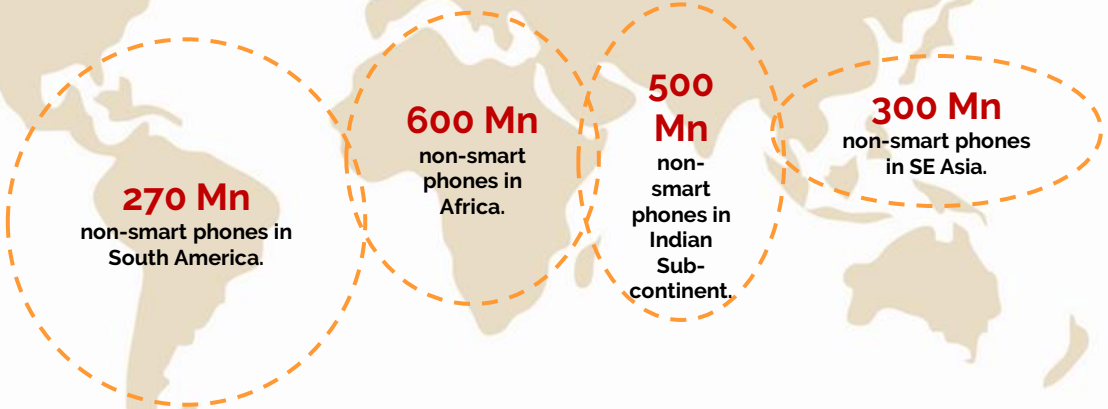
Hungry for a secure & easy to use service and adopt the services

1.67 Billion Non-Smartphone Users in Target Regions

Region	Non-smart Phones	Smart Phones
Indian Subcontinent	62%	38%
Sub Saharan Africa	69%	31%
S E Asia	58%	42%
Central & South America	44%	56%

Need of the hour :

- Security
- Trust
- Simplicity
- Ease of use
- Local language



A mobile may not be as “strong” as you think

- Was built for voice and messaging
- NOT FOR SECURE PAYMENTS
- Missing is :
- Security / encryption / trusted environment for payments / credential storage / keys and more

Smart phones :

App strength

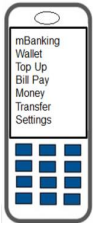
Android OS

As “strong” as the OS – can confirm this for the large / organised device companies

Smaller / local companies ???

Non-smart phones :

- **OS - ????**
- **App hosting credibility - ???**
- **Installed apps – cannot update**



Growth of financial services to the masses :

BUILD TRUST / CONFIDENCE AND SECURITY IN THE TOTAL SOLUTION

What actually happens

OTP "Hijacking"

- OTP delivered into the SMS IN-BOX, read by another malware, "transported" over SMS / data to another mobile / mail address (remember you gave permissions to apps to Read / send SMS)

All **SMS / USSD messages are in open text at the operator console**, with all data parameters available to read. Just change the amount / destination !!!

Storing login / secure credentials

- In the mobile app, unsecured OS lets a malware "crawl" through the OS and read another app data (android 7.1 and beyond only gave software security, no hardware security)

SIM cloning :

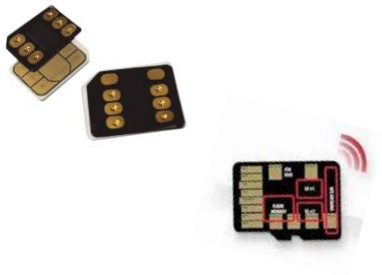
- "hijack" the MSISDN, call the bank for "forgot password/PIN" new PIN delivered to the new SIM and you have full account control

The future …. How do you handle Crypto currencies / Bitcoins / digital currencies / secure access credentials for anything

The non-smart mobile user is the most vulnerable, not that the smart phone user is less

What NextGen Offers

Power mobiles with secure environment for digital banking & payments



SIM overlay + secure MicroSD card

Product highlights (trust and security)

- Banking | bill payments | top up
- Money transfer
- Merchant payments
- Cash-in | Cash-out
- **Card less | contactless ATM cash withdrawal**
- Loans & Insurance
- Secure token / crypto hosting

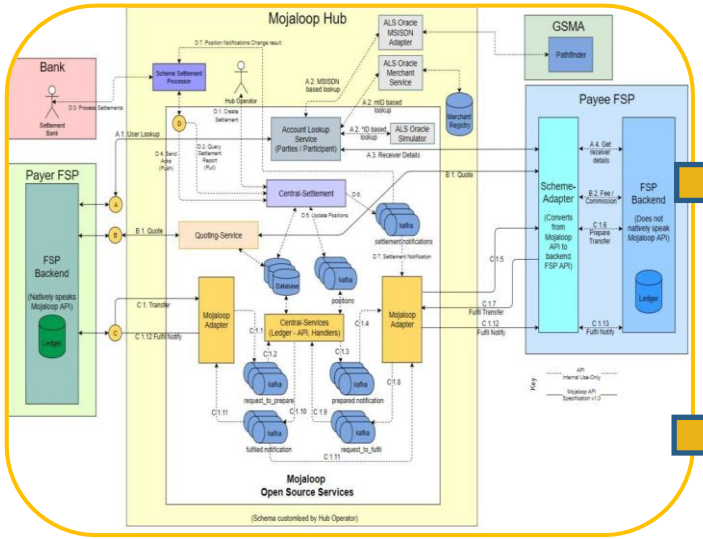
Simplified Customer on-boarding – KYC must

- Retail agents
- Mobile retail shops
- Bank branches

Simplified Activation

- Validated against issuance parameters with switch
- If OK, secure tokens installed Over The Air
- Good to go

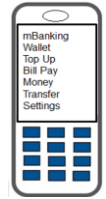
The NextGen Service Bridge



Mojaloop Hub

The Service Bridge over SMS

- Issuance
- Banking / Wallets / P2P / P2M / bill and utility payments
- Micro Finance / Insurance
- Customer / agent banking
- Cash IN / OUT
- Crypto / digital currency

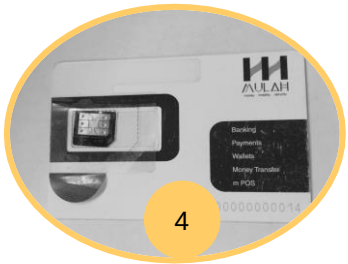


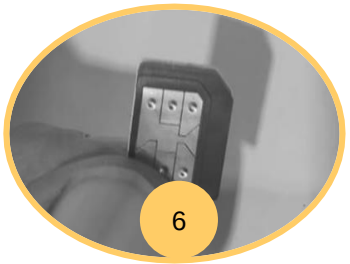
The Service Bridge over Data

- EMV / DESfire card hosting (Visa / masterCard)
- Crypto currency / Digital Currency
- NFC to any mobile

How We Do it – Overlay Solution

Paper-thin SIM overlay film with a micro chip, pasted on existing SIM & inserted into SIM slot.
Application sits on overlay & enables a simple, user friendly, multilingual & secure service menu





How We Do it – Secure microSD card / POS / QR

Merchant NFC Mobile :
- Add Contactless card acceptance
- Add payment QR code capability

Customer mobile :
- Android : add NFC capability (SD card)
- Read payment QR code

Accept NFC and QR code payments

Un-organised retail / small shops

Merchant Billing POS :
- Add payment QR code capability

Customer mobile :
- Android : add NFC capability (SD card)
- Read payment QR code

Add QR code capability
Traditional POS – accept NFC payments

Organised retail / large outlets

Solution Highlights

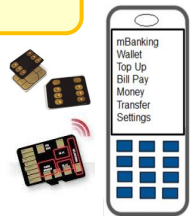
moja =one (SWAHILI)
one loop
for everyone

Mojaloop Central Switch

Customer on-boarding :

- Map MSISDN + IMEI + hardware Sr# to customer credentials (KYC / ID / card / bank ID)
- Secure tokens issued / mapped, and OTA loaded into the "chip"

Mobile / Web UI – simple



Device security :

- Enhanced with secure element
- Remote secure update for tokens / crypto currency / credentials / login access

No- Hijacking / SIM cloning

Transactions

- Encrypted / decrypted at both ends
- Public + private keys
- SMS and data channel

Security

- Multi factor authentication – Login PIN + token validation + Txn PIN
- Unique key per chip
- HSM integrated

Multi factor authentication

System Flexibility / Strength :

SIM overlay

- Hide / unhide menu listing
- Remote Over The Air (OTA) updates for data (billers list / token)
- Secure OTP – encrypted and within the overlay
- Secure token OTA loaded – added validation
- Crypto currency / digital currency / tokenized cards
- Android integration – Q1 2021

MicroSD Card

- Add NFC to any device
- EMV card hosting directly on SD card (credit / debit / pre-paid / stored value)
- DESFire cards (transit / localized payment)
- Regular SD card storage (8 /16 / 32 GB)
- Integrates with any android app

Banking Grade Security / Encryption / Storage

Secure Element (SE)

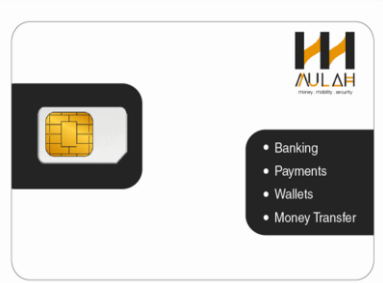
- Unique encryption / decryption key for each element – 128 bit
- 3DES2.0 / AES engines and secure data storage area
- Mapped to customer Mobile# / IMEI and software version
- Data storage on SE/ MicroSD card is secure and encrypted
- EMV / PCI 1.0 / EAL4+ certified
- Add NFC to any device – smart and non-smart

Platform

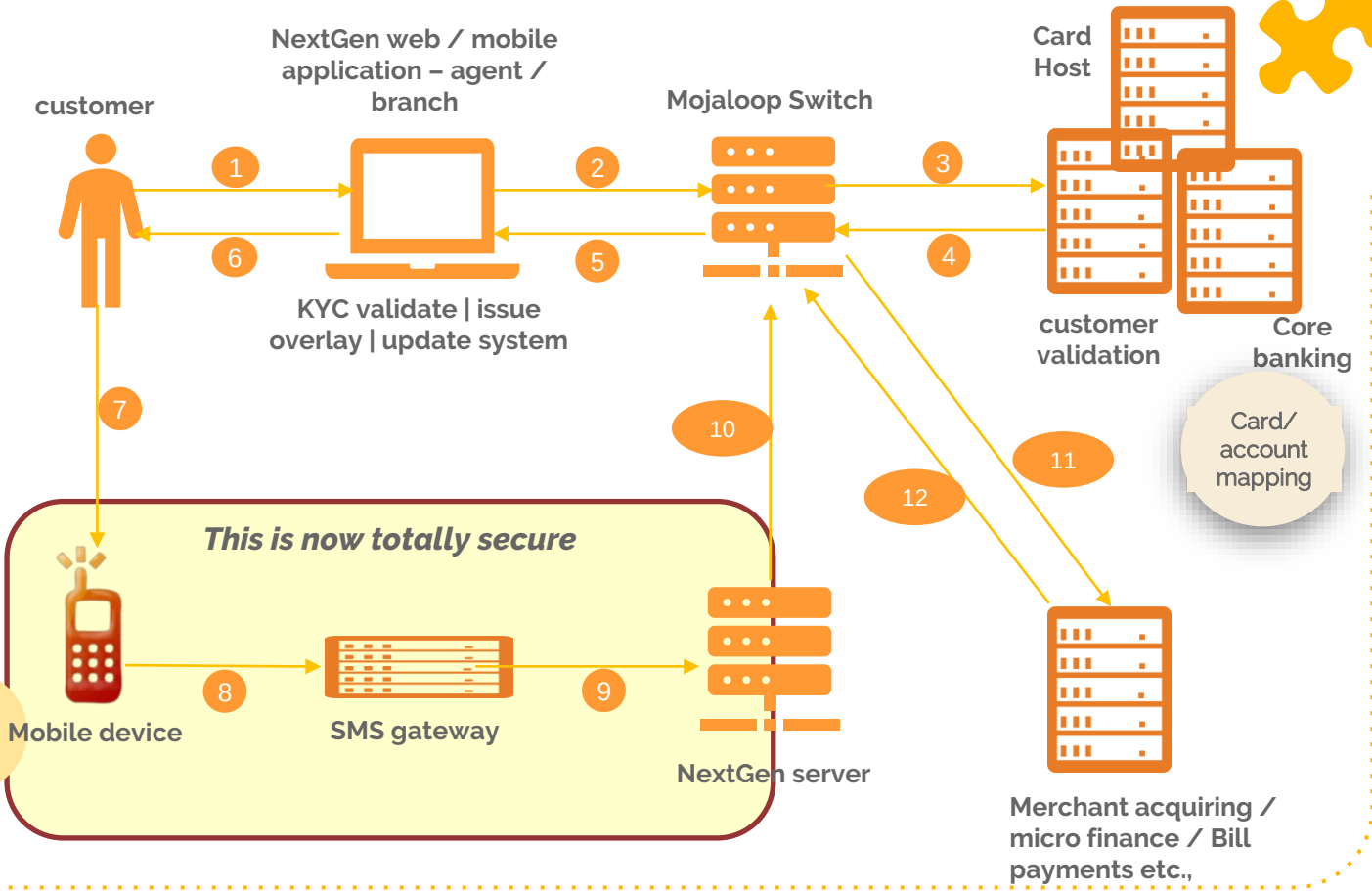
- Banking grade PCI / DSS certification in place
- Advanced data encryption using Hardware Security Modules
- Secure firewalls and limited access allowed

Data transmission

- Unique encryption for each data string
- Multiple customer issuance mapping parameters for request validation
- Internal checks for multiple requests

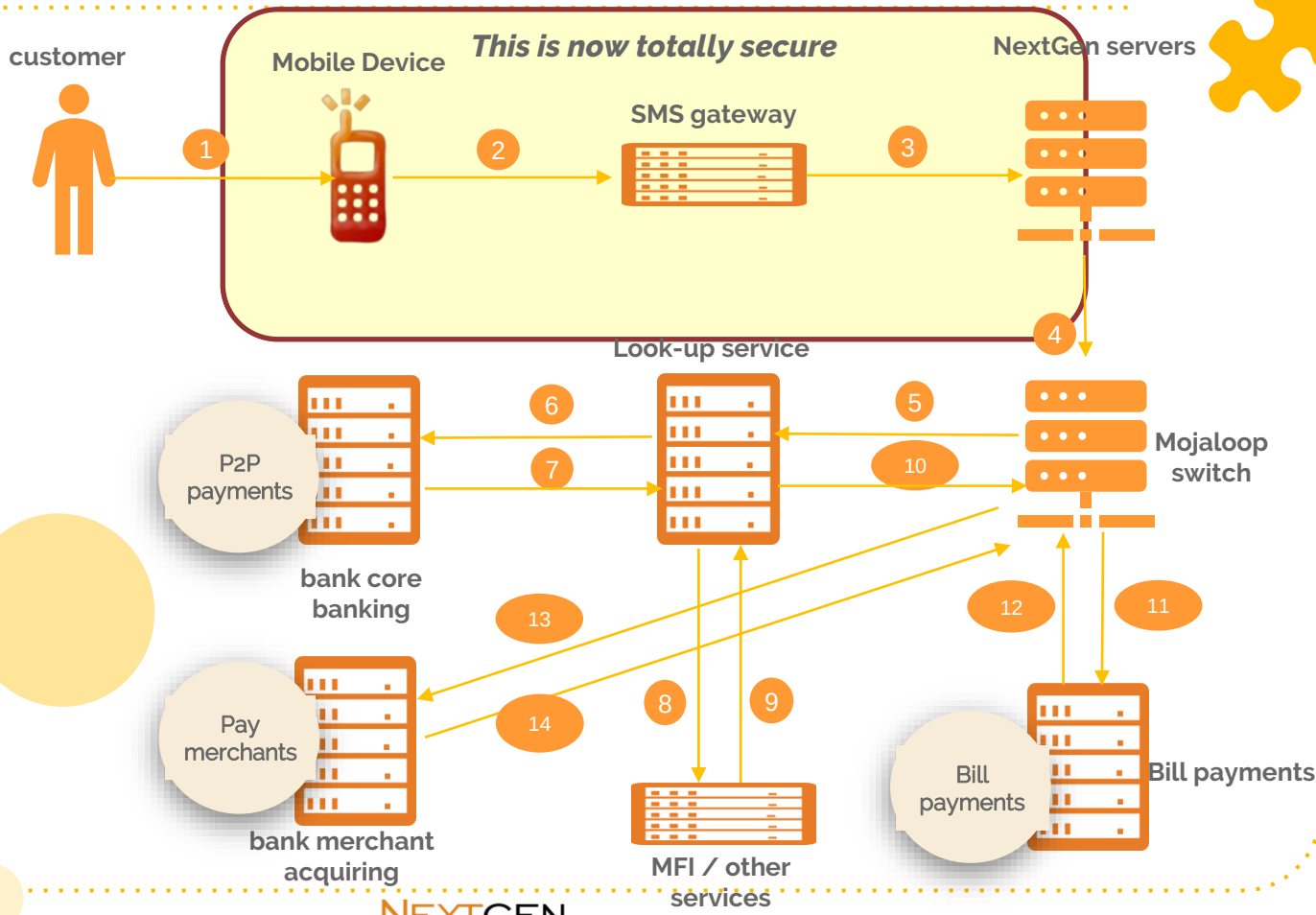


Process Flow SIM Overlay Issuance & Customer Registration



Process Flow for Transaction Using SIM Overlay

Banking | P2P| P2M | Bill Payments



The Partnership… what it brings ?

A “Trusted Execution Environment” to any mobile

What it now gives…

Regulators / banks / central governments :

- Helps “build / convey” trust and security in the country’s digital financial services ecosystem
- Catering to every user segment – and more to the masses on non-smart phones
- Helps build the Foundations for adopting future crypto / digital services with peace of mind
- Security at every step :
- On-boarding / credential storage / KYC management / transactions

Scheme partners / service partners :

- Takes away the “technology challenges”, leaving them with pure service designing, marketing and generating revenues / traffic
- Brings in multiple service verticals – interoperable and integrated
- And future proof

mojaloop foundation

NEXTGEN

Thank You !

For more information, please get in touch with Mojaloop or NextGen