Mobile Connect Summit Singapore

21 & 22 November 2017

Suntec Exhibition & Convention Centre, Suntec City

Emerging trends and disruptive technologies in digital identity

Jaikishan Rajaraman

Global Head of Technology, GSMA

A global, standardised authentication, identity and attributes service framework

Authentication

Simple and globally ubiquitous **log-in**

- authenticate
- authenticate plus

Authorisation

User **authorisation** of SP requests

- authorise
- authorise plus

Identity

Provision of user **identity**

- phone number
- sign-up
- national ID

Attributes

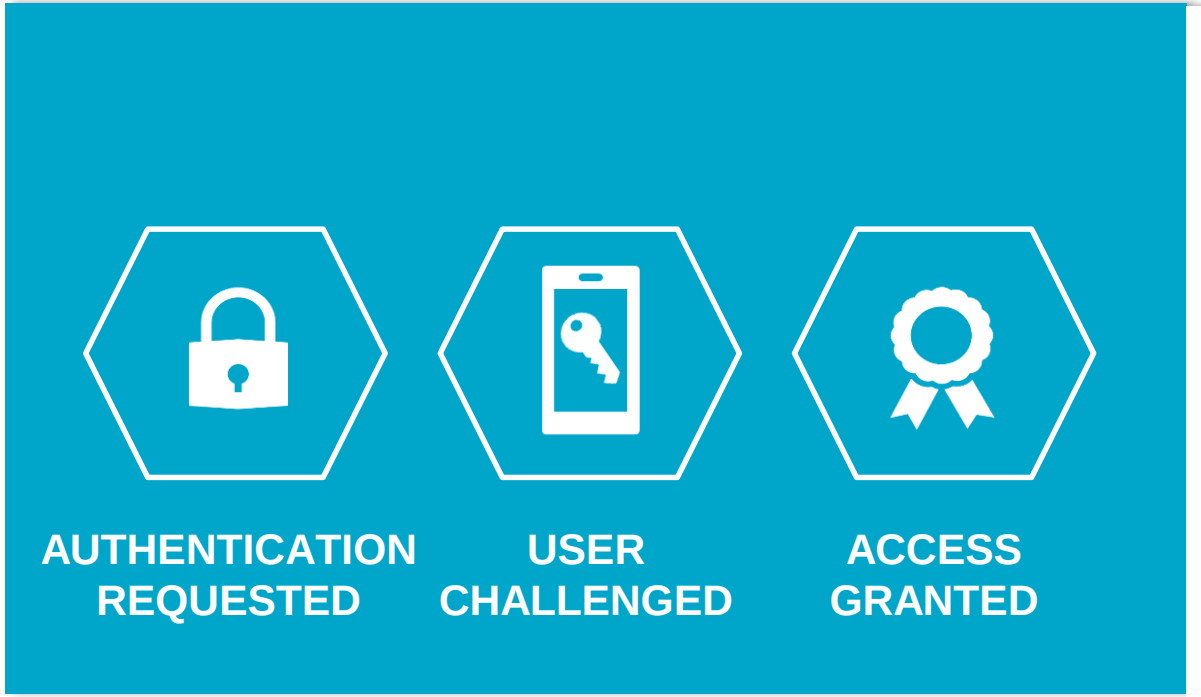
Insights about the **user**, **device** or **transaction**

- KYC match
- account takeover protection
- verified MSISDN

Helping users manage their identity across their **digital footprint**

Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

Authentication
Simple and secure user authentication on a global scale



Use cases

- Universal password-less login
- Convenient 2-Factor authentication
- Hard token replacement

Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

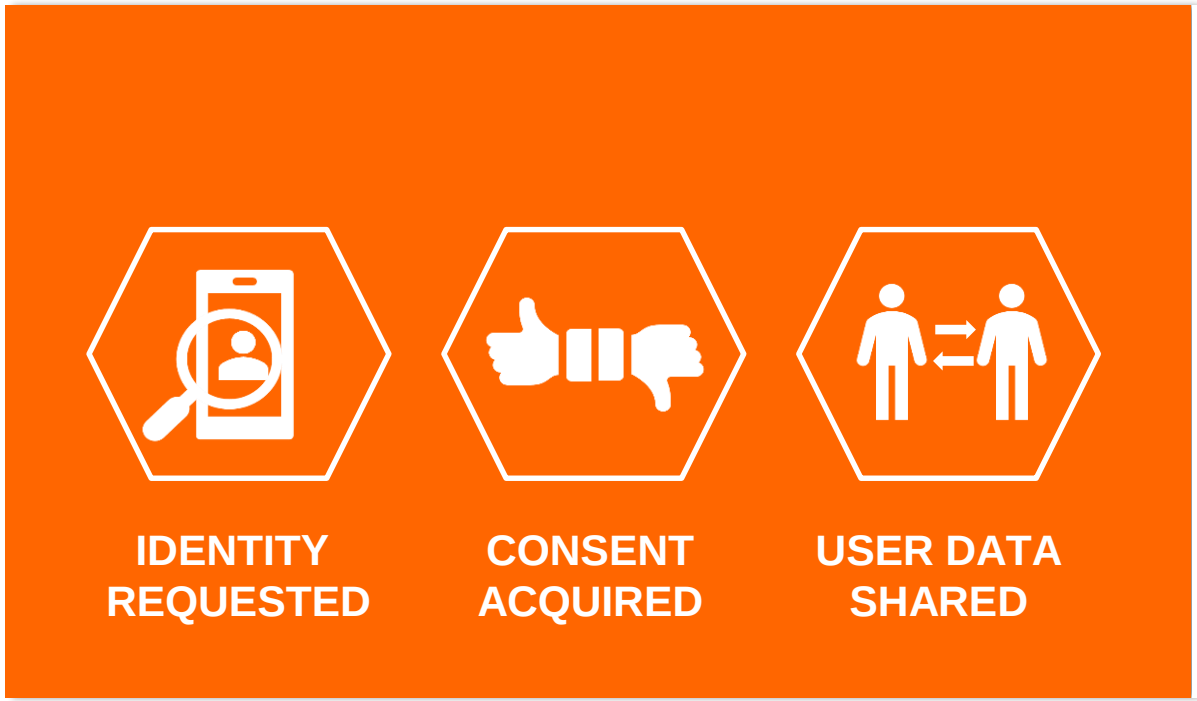
Authorisation
Contextual & explicit approval through a mobile device

Use cases

- Payment approvals
- Parent approval of child's purchase
- Simple captcha replacement

Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

Identity
Verified personal data retrieval with user consent



Use cases

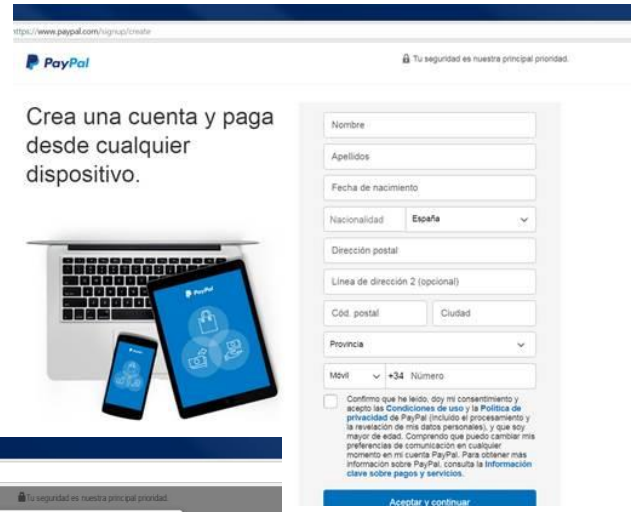
- Provision of user's phone number
- One click signup & guest checkout
- Regulatory compliance ID checks

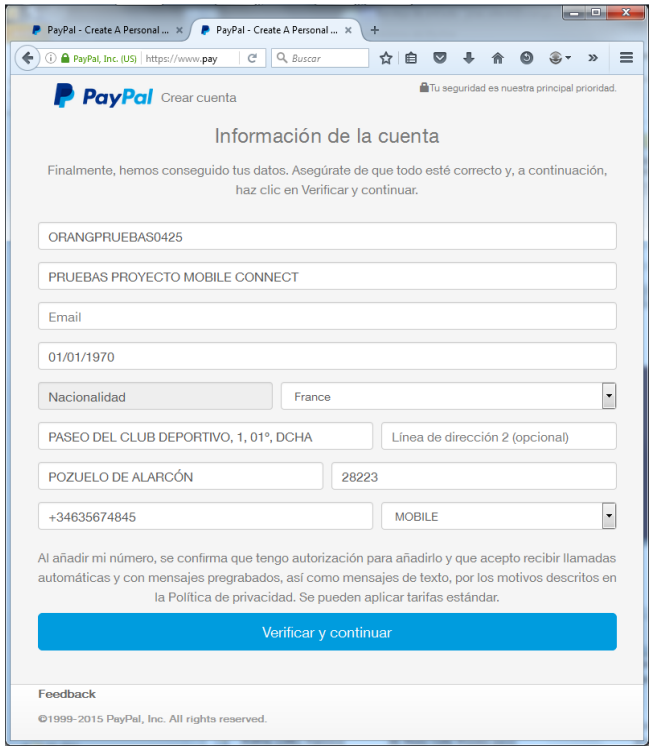
Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

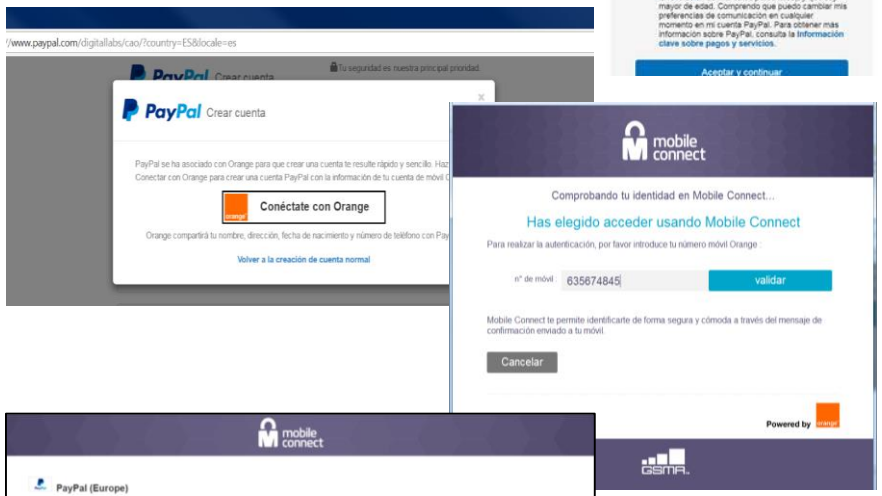
Identity: Orange and PayPal

Sign-up to use PayPal in France & Spain

- Create your Account with PayPal
- Select to connect with Orange
- Enter mobile number to authenticate
- Accept terms & conditions
- View and verify your details to make the transaction







Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

Attributes
Mobile subscriber checks for ID verification & fraud mitigation

Use cases

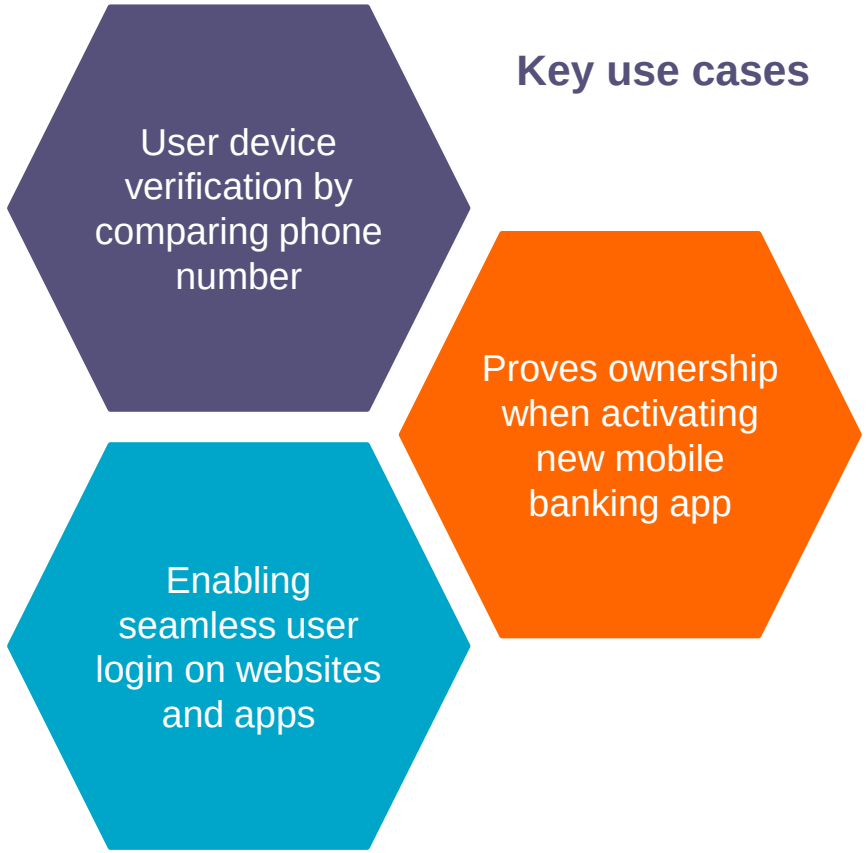
- KYC information check
- SIM swap fraud prevention
- Seamless device verification

Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

Mobile Connect Verified MSISDN

- Seamless user device verification
- Service Provider receives the phone number associated with the mobile device accessing their online service
- Highly secure data from the network (cannot be spoofed by device malware)
- Works with devices whilst on mobile data network
- Supports invisible authentication experience when used with SP pre-stored phone number
- Single API from multiple operators globally

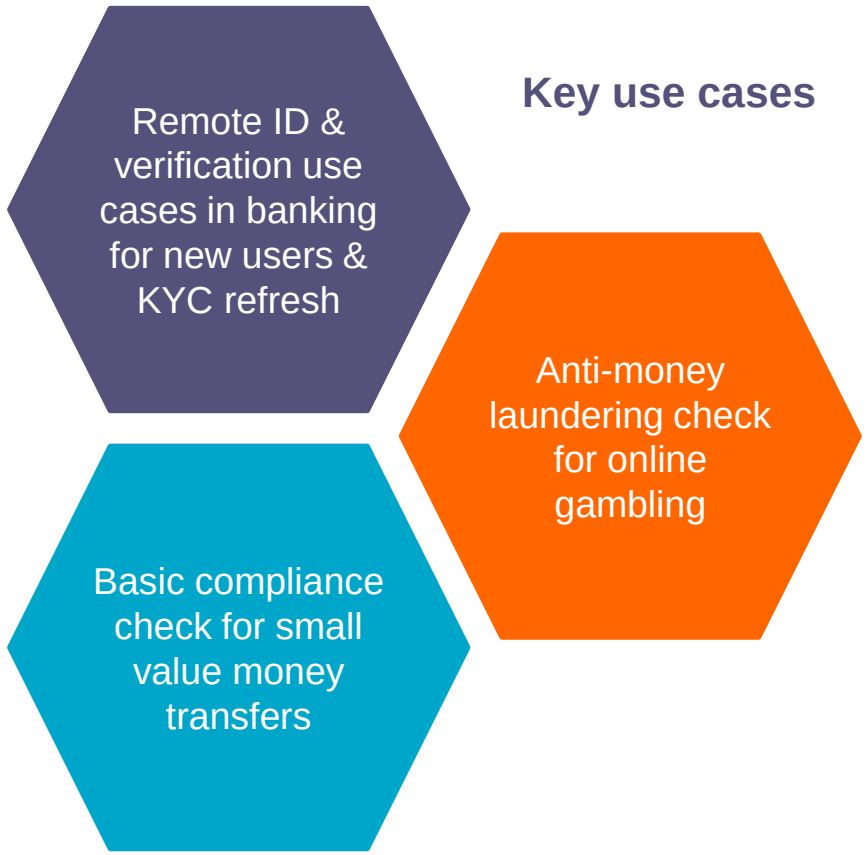
Key use cases



Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

Mobile Connect KYC Match

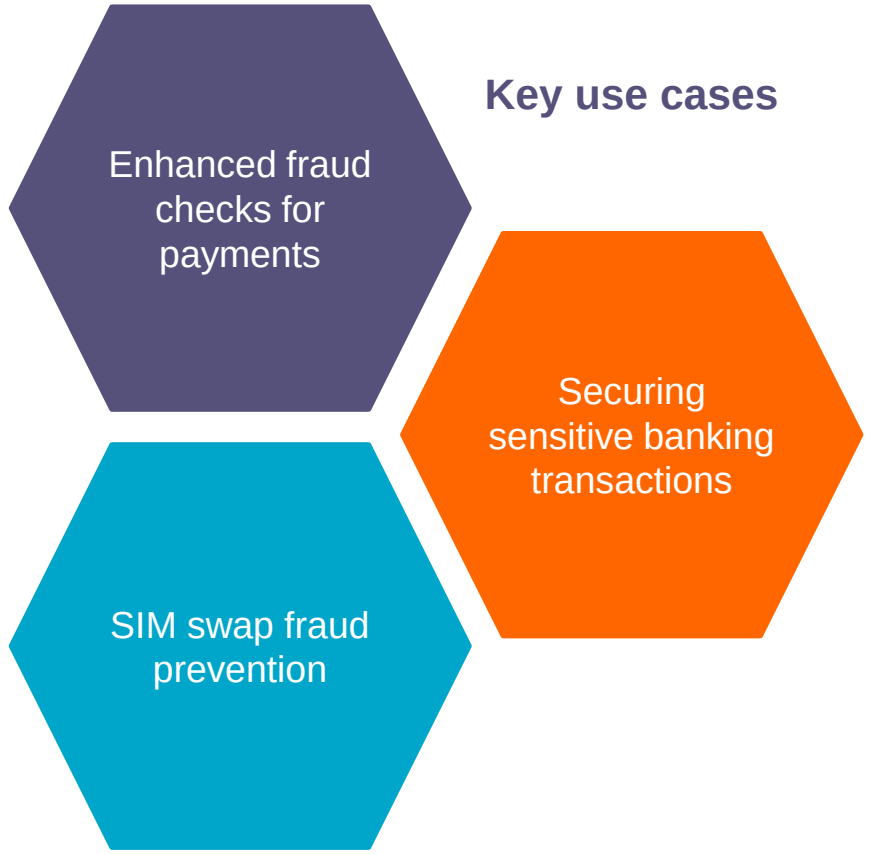
- Straightforward User ID verification
- Service Provider receives comparison of the user's name and address relative to the information held by the mobile operator
- Hashed data or plain text data matching options
- Flexible to support different consent models
- User interaction or background processing modes
- Single API from multiple operators globally



Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

Mobile Connect Account Takeover Protection (ATP)

- Helps spot fraud in online services that use the mobile phone for 2FA
- Service Provider receives information on the pairing between a user's mobile phone account and their device (i.e. last SIM change date and active call divert status)
- Verified data from the network (cannot be spoofed by device malware)
- Helps prevent SIM swap fraud
- Single API from multiple operators globally



Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

Attributes: KYC match (Fraud reduction)
Bank Use case – to be launched in the UK

Customer adding a new beneficiary via his desktop.

Customer select preferred mobile number for contact

Automated Call is placed to customer, which plays an IVR.

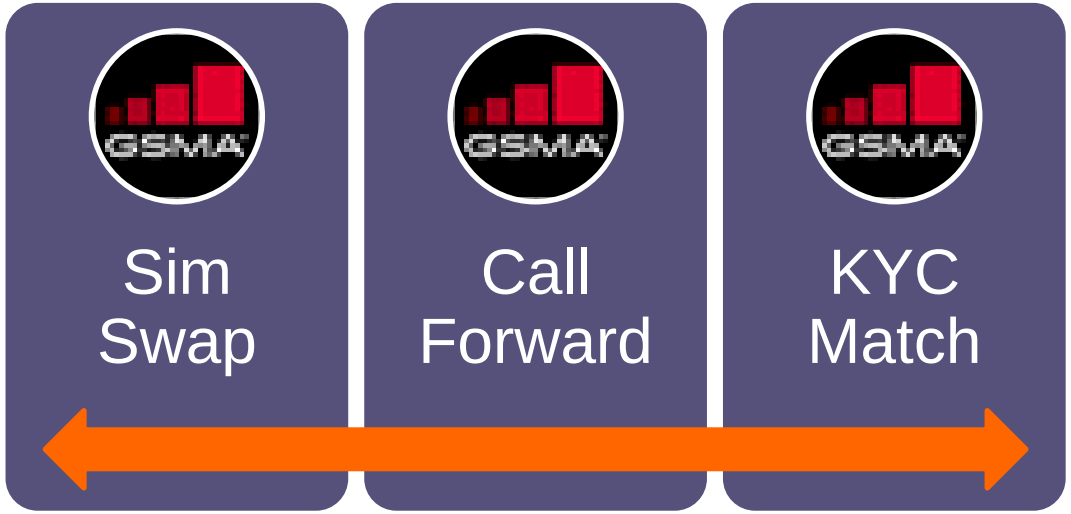
User is provided a 6 digit number to enter it on their mobile keypad

Transaction processed on receipt of correct PIN

Transaction ends

Once the Customer chooses a mobile number to be called, the system calls the Mobile Connect API and checks three elements.

Bank can enhance the check by having access to the location of the handset to ensure it corresponds with the location of the desktop.



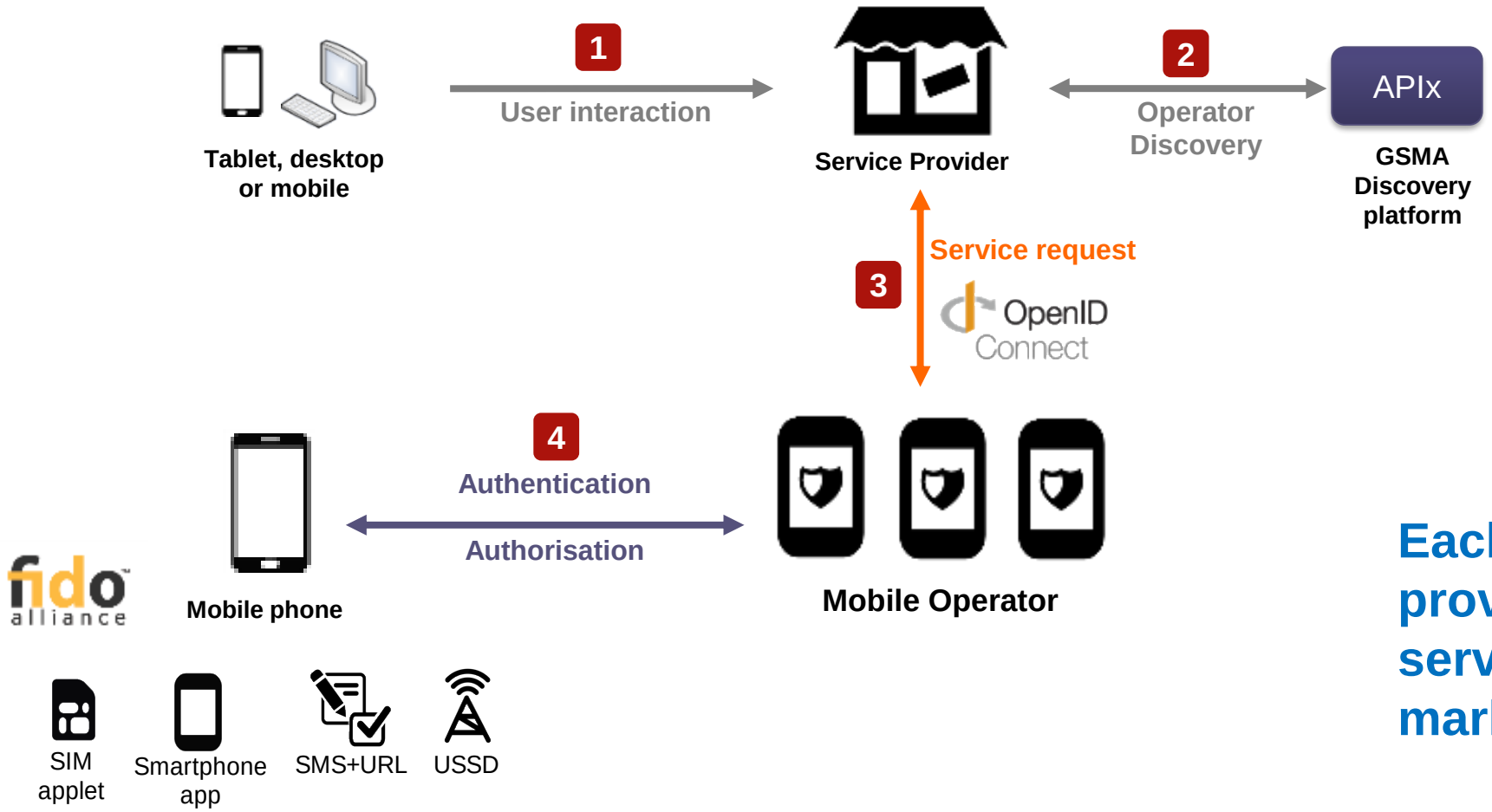
Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

Selecting authenticators

		Pros	Cons
USSD		• Works on all phones • Doesn't require data connections • Secure channel	• Requires user input • Can take time loading • Displays differently on different devices
SMS/URL		• No user input required • Works consistently across enabled devices	• Low security • Requires data connection • Data charge may discourage users
SMS/OTP		• Works consistently across enabled devices • Works on every single phone	• Not secure • OTP requires User Input • 8 step process
SIM Applet		• Super quick and secure (esp. for LoA3)	• Limited text strings for UX display • High investment to roll out
Smart Phone App		• Very smooth UX as eliminates call times and processes	• Only available for smartphones

Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

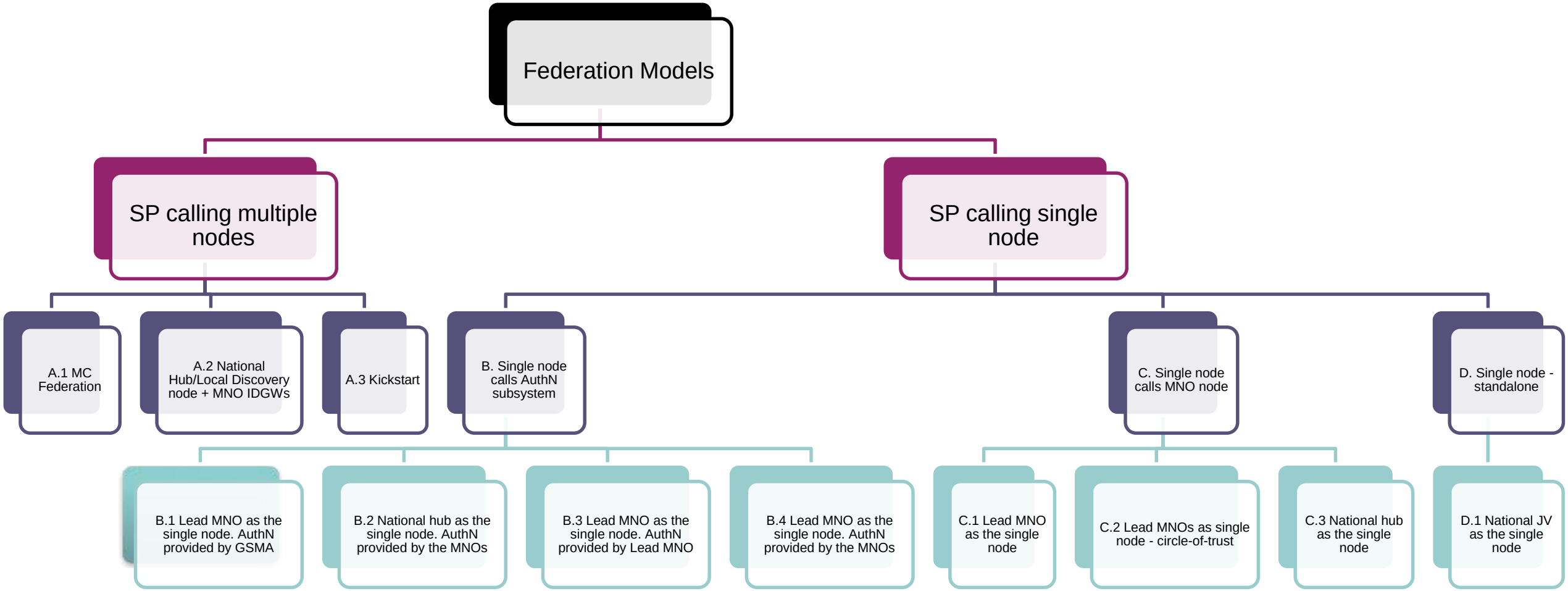
Mobile Connect high level architecture



Each MNO required to provide Mobile Connect services to deliver full market coverage

Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

Mobile Connect Federation Models



Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

Next steps – Taking Mobile Connect to the market?

Evaluate market opportunity

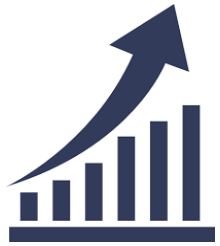
- Mobile Connect enables operators to provide authentication, authorisation, digital identity and attributes in digital services

Define commercial strategy & business case

- Mobile Connect requires low capital investments and is a relatively easy deployment
- To succeed: scale fast and overcome industry fragmentation

Deploy interoperable architecture

- Mobile Connect architecture's 3 key parts: Authentication mechanism; ID Gateway; Discovery service (API Exchange)

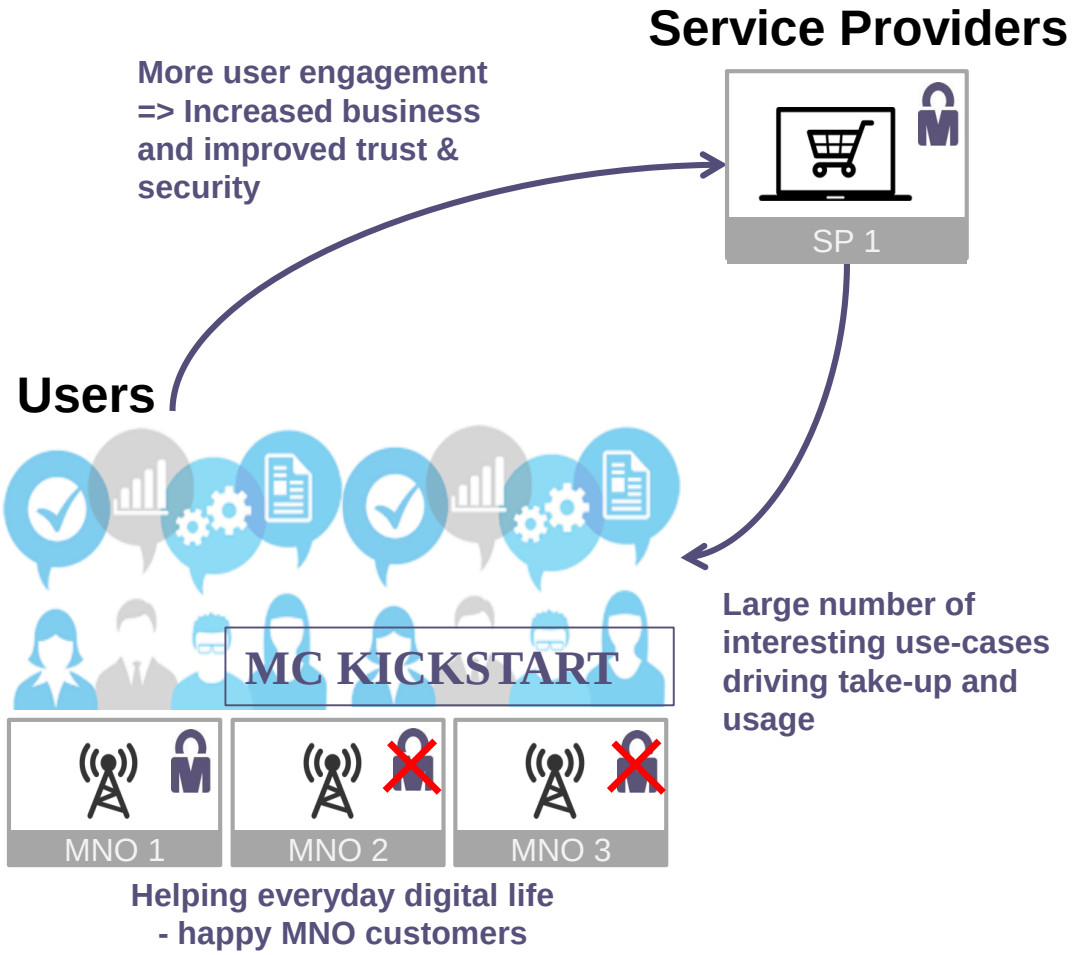


Grow take up and usage

- To scale Mobile Connect, operators need to work on both increasing end user awareness and on deploying with external SPs

Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

GSMA Mobile Connect Kickstart: User coverage is key



- Service Providers (SPs) are operator-agnostic, and need ubiquity of access for their users
- If all operators are not ready at the same time, SPs are reluctant to deploy MC, leading to fewer services and therefore fewer active users
- GSMA Mobile Connect Kickstart allows operators to immediately have their customers be discoverable and hence be authenticated using MC – this provides a favourable SP proposition
- Examples: Digi (Malaysia), Telefonica (Colombia, Peru, Argentina)

Copyright © 2017 GSMA. The Mobile Connect logo is a trade mark registered and owned by the GSMA.

WSO2.Telco

Mobile Connect for Longtail APIs

Digital Enablement Powered by APIs for Telcos

About WSO2.Telco

WSO2.Telco products enable Mobile Network Operators to leverage existing infrastructure, implement additional revenue streams and remain relevant in the digital age.

Telco Innovation + Visionary Platform + Community engagement = Digital Transformation for Telcos

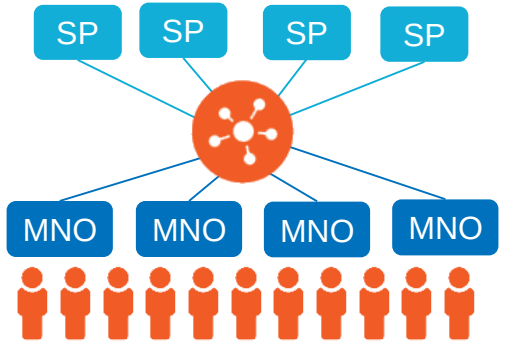
Copyright © WSO2.Telco. All rights reserved.

Our Vision

Shorter Product Release Cycle

1000s of Partnerships

Exponential Reach

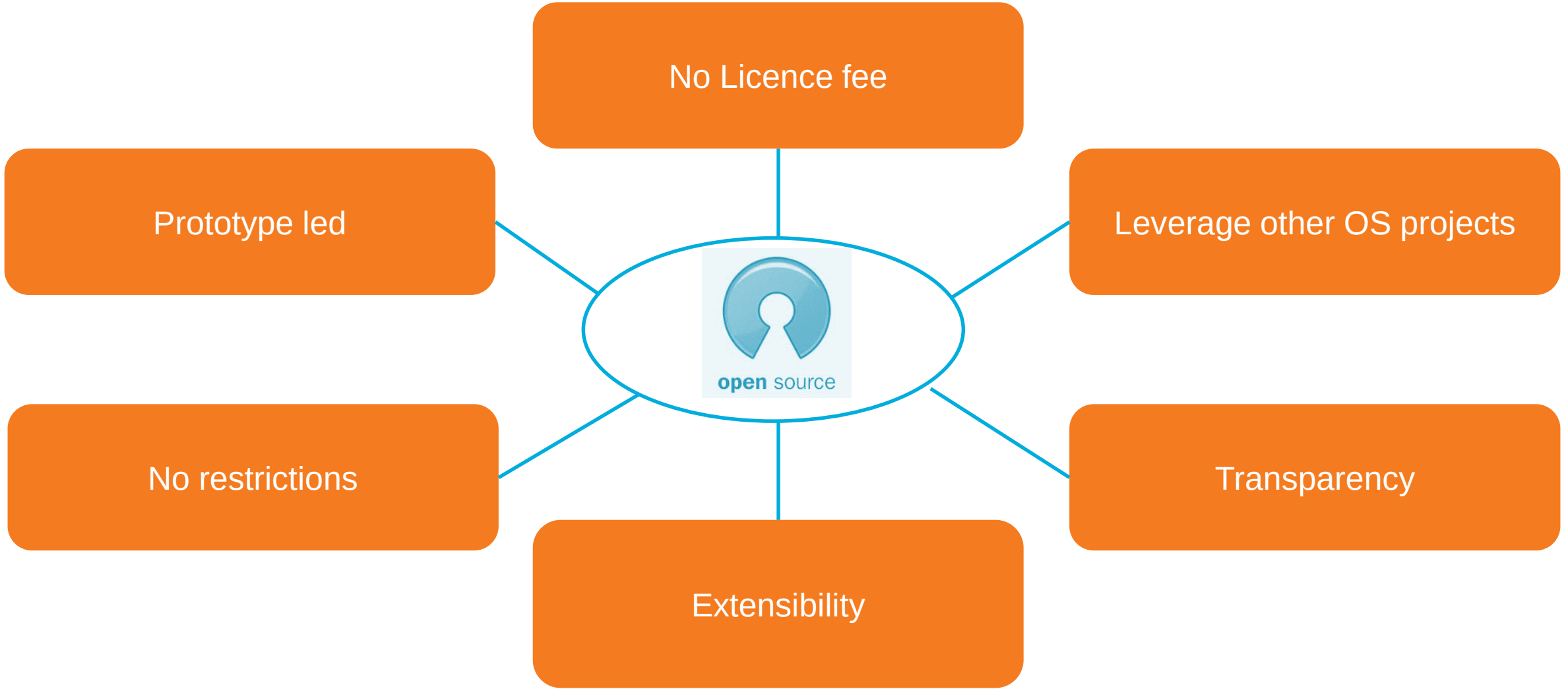


Optimize Operational Efficiency

New Revenue Through Innovation and Access

Copyright © WSO2.Telco. All rights reserved.

Why Open Source?



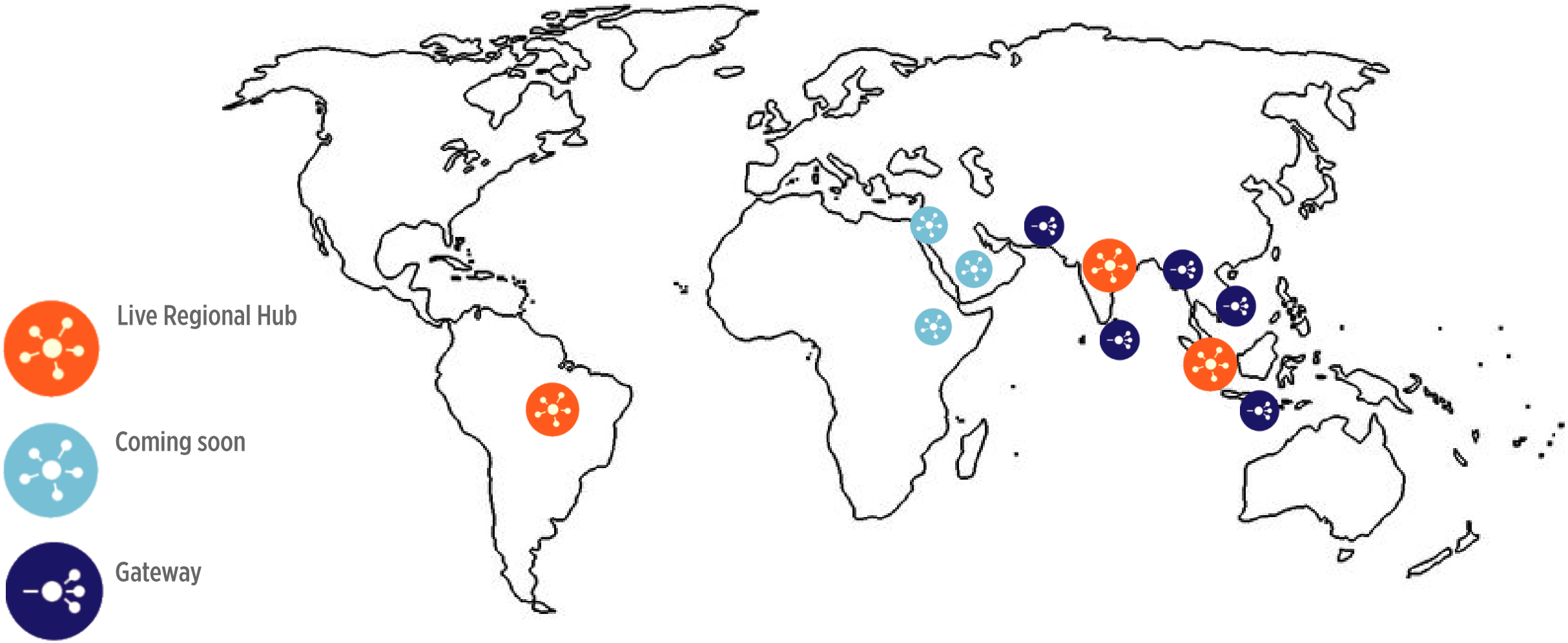
Copyright © WSO2.Telco. All rights reserved.

Digital Enablement Platform

KEY REFERENCE CASES

Copyright © WSO2.Telco. All rights reserved.

Our Deployments



Copyright © WSO2.Telco. All rights reserved.

Axiata Internal & External Enabler

320 M Subscribers

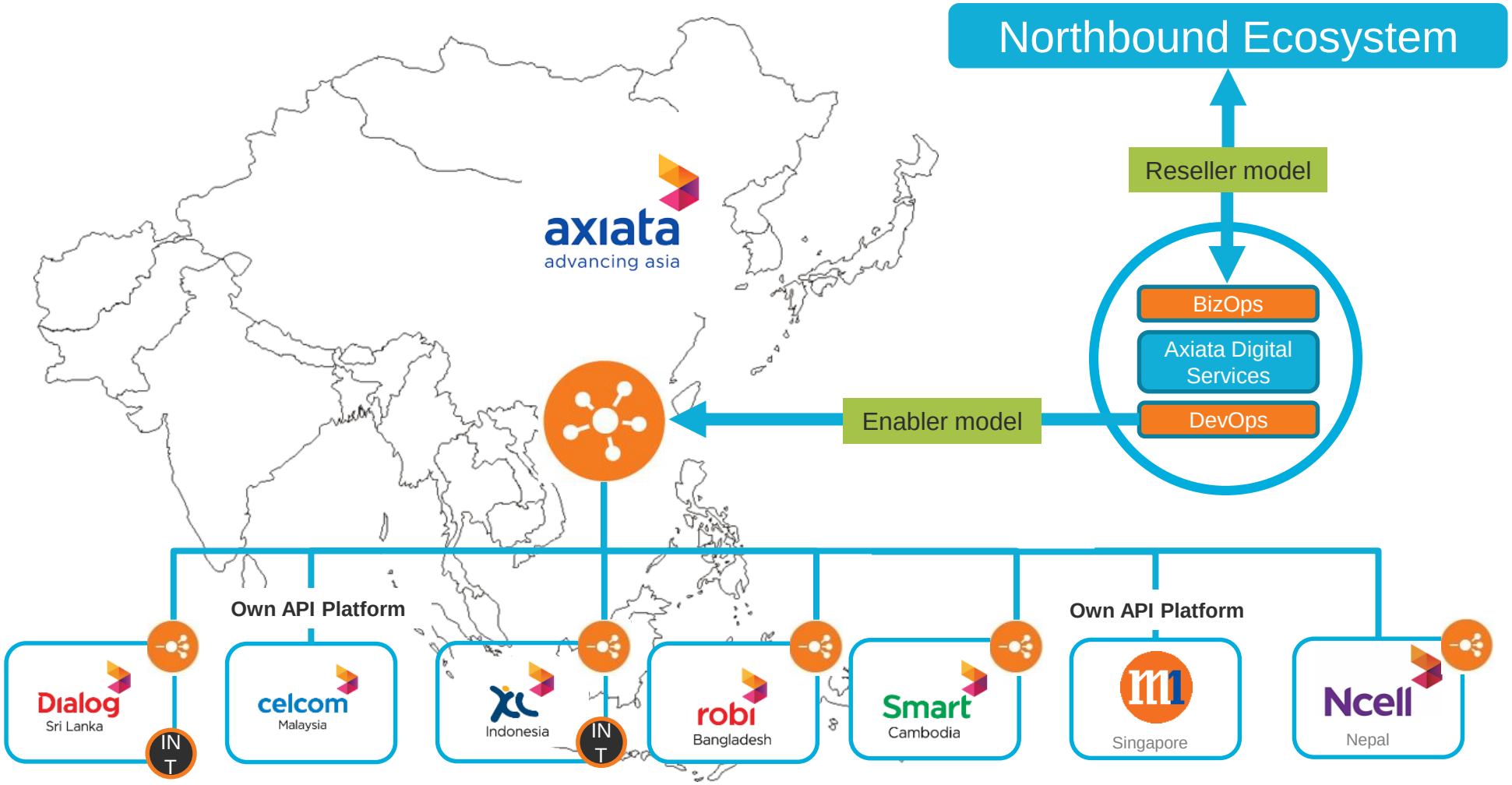
enterprises
developers
telcos

Lets partner & innovate

1 Integration
Single point of contact

Leverage our infrastructure

Connect to our customers



Hub

Gateway

Internal GW

Copyright © WSO2.Telco. All rights reserved.

TELCO SERVICE SUBSCRIPTION

Copyright © WSO2.Telco. All rights reserved.

Why Consent Management?

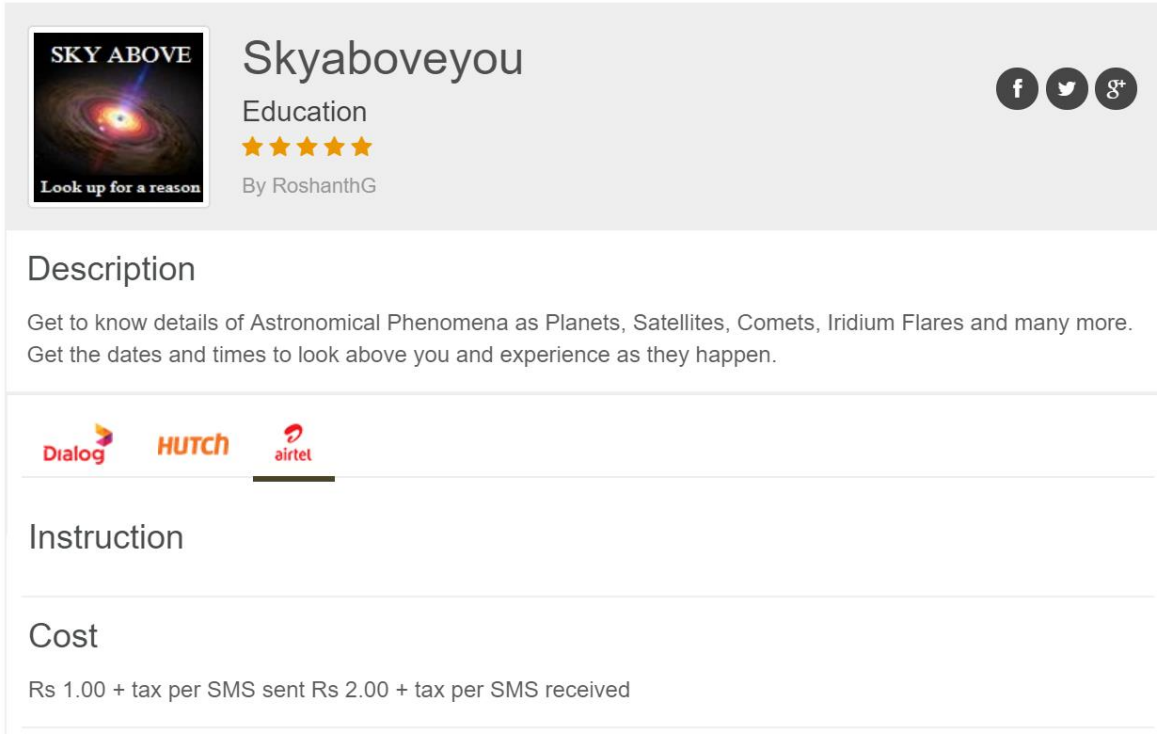
- Unethical content subscription
  - High complaints
  - Fraudulent activities
- Regulatory concerns
- Privacy violations
- Service provider monitoring and tracking
- Complex Subscription engines

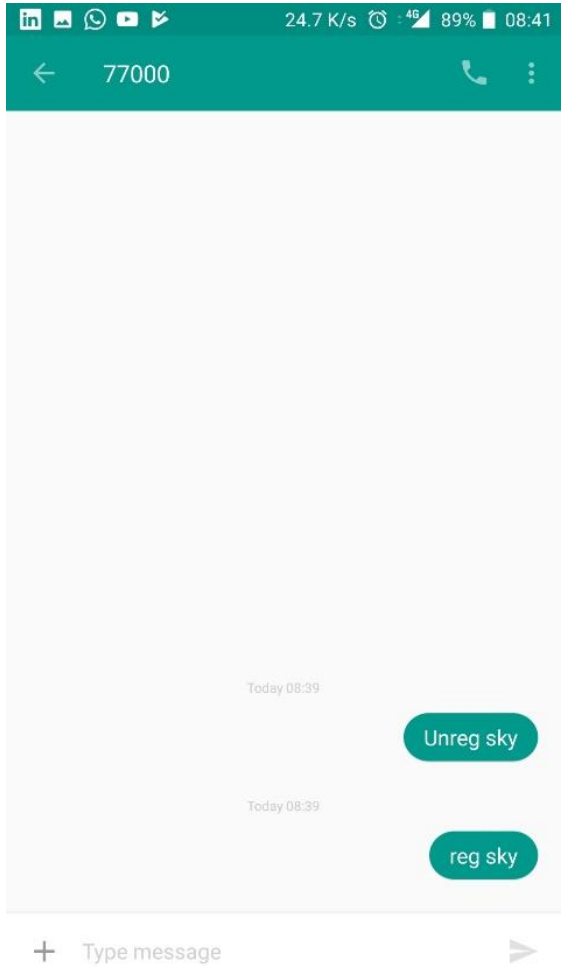
Telcos limited to trusted partners

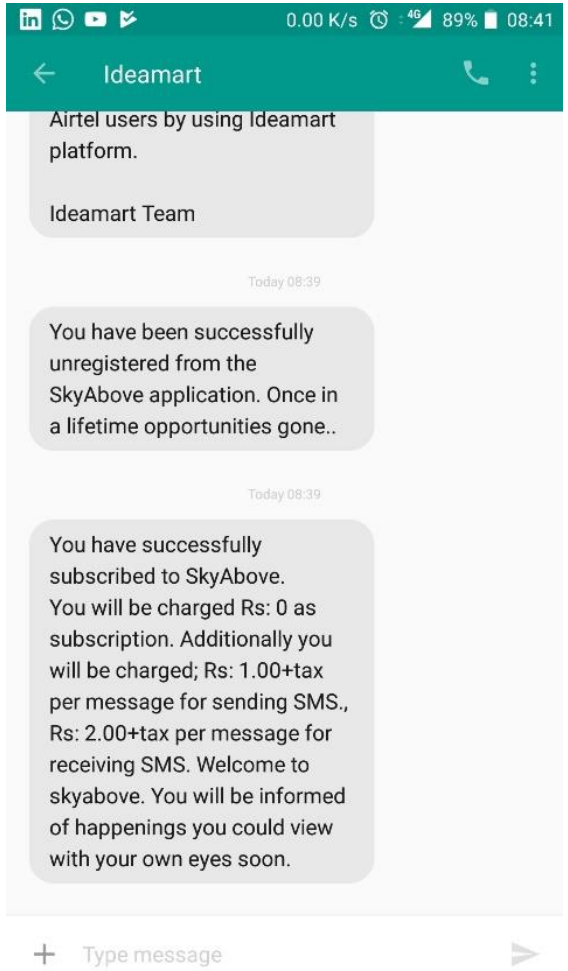
Copyright © WSO2.Telco. All rights reserved.

Traditional VAS Services

- SMS or USSD Based Service Subscription



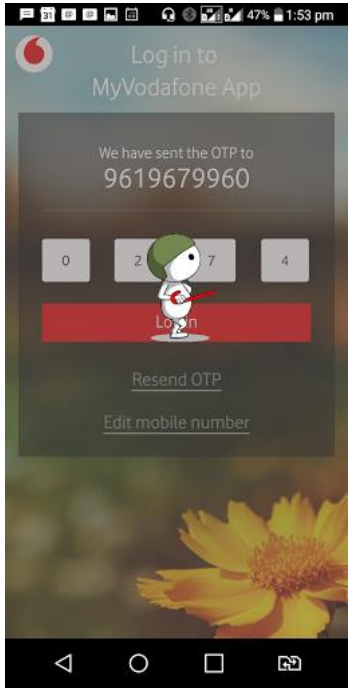


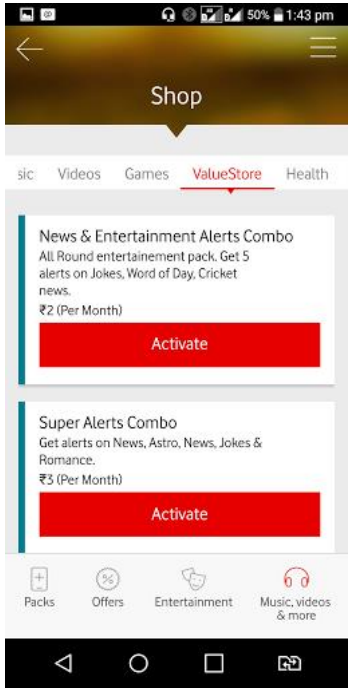


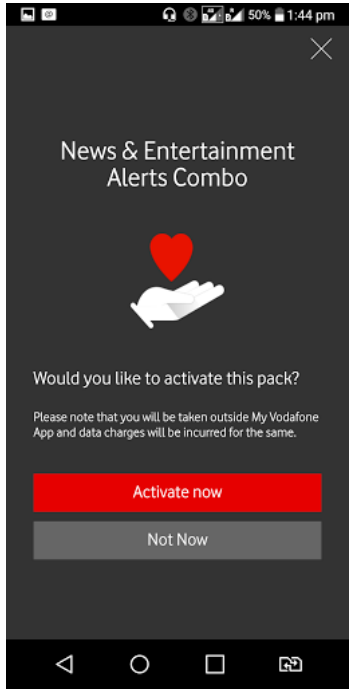
Copyright © WSO2.Telco. All rights reserved.

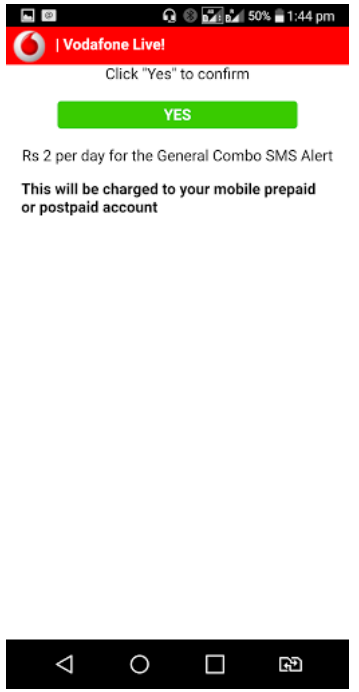
DoB Consent and Consent Gateways

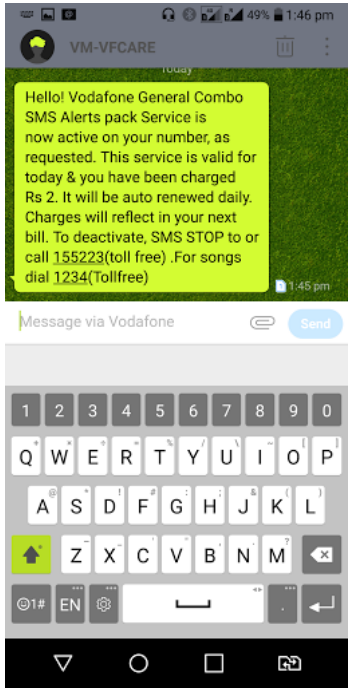
- Smartphones and online portals











Copyright © WSO2.Telco. All rights reserved.

Download VLC Media P

Not secure | filehippo.com/download_vlc_media_player/32/

FILEHIPPO
Software That Matters

Search Software

Windows | En

DOWNLOADS | BUSINESS SOFTWARE | NEWS | REVIEWS | TOP APPS

Home › Windows Apps › Audio and Video › Players › VLC Media Player

Share | Tweet | Share

VLC Media Player 2.2.6

By VideoLAN.org (Open Source)

User Rating

Download 32 bit (29.52MB)

Advertisement

START DOWNLOAD

3 Steps to Track Your Package
1. Click 'Start Download'
2. Free Access - No Sign up!
3. Get Tracking Details

PackageTracer™

Advertisement

START NOW

3 Steps to Track Your Package
1. Click "Start Now"
2. Free Access - No Sign up!
3. Get Tracking Details

PackageTracer™

Description | Technical | Change Log | Comments

VLC Media Player is the most popular and robust multi format, free media player available. The open source media player was publically released in 2001 by non-profit organization VideoLAN Project. VLC Media Player quickly became very popular thanks to its versatile multi-format playback capabilities. It was aided by compatibility and codec issues which rendered competitor media players like QuickTime, Windows and Real Media Player useless to many popular video and music file formats. The easy, basic UI and huge array of customization options have enforced VLC Media Player's position at the top of the free media players.

Notify me when this program is updated

Cookies help us to deliver our services. By using our services you agree to our use of cookies. More info

Okay

filehippo.com/download_vlc_media_player/32/#null

Menu | Downl... | conf | amila... | [amila... | [*Uns... | amila... | MySQ... | comp... | amila... | comp... | [Down... | root@... | Downl... | 12:38 AM

Mobile Connect for Long Tail APIs– Our Approach

Choice of Authenticators

User Dashboard

Audit Trail

Mobile Connect Authorize Product

API Management

RFC 7662

Copyright © WSO2.Telco. All rights reserved.

Why MC for Managing Consent

- Consistent view and complete control for customer
  - Traditional Services VAS services
  - Internet Services
  - Manage Service on an ongoing basis
- Complete Transparency for end users
- Consistent developer experience for service providers
  - Global Reach
- APIs for long tail developers
  - Minimum risk and highest security
  - Ensure audit trail and

Copyright © WSO2.Telco. All rights reserved.

PLEASE CONTACT US

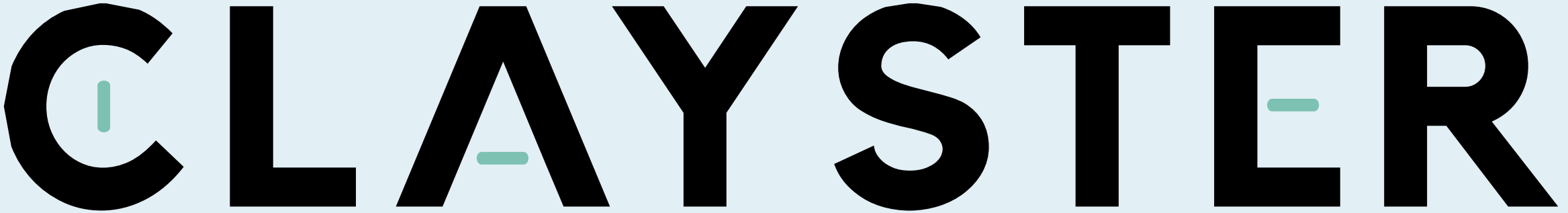
Our Contact details	
Technical	
▪ Gaya Dahanayake ▪ E: gaya@wso2telco.com ▪ M: +94772565151	
Commercial	
▪ Mirantha Perera ▪ mirantha@wso2telco.com ▪ +94777571026	▪ Liara Ibrahim ▪ liara@wso2telco.com ▪ +94777123392
Support	
▪ Yumani Ranaweera ▪ E: yumani@wso2telco.com ▪ M: +94 777795242	

www.wso2telco.com

Email: info@wso2telco.com

Copyright © WSO2.Telco. All rights reserved.

CLAYSTER


CLAYSTER

SOMETHING

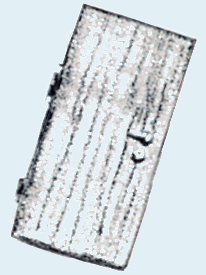
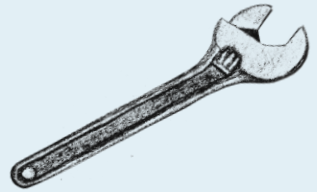
What does it mean to own

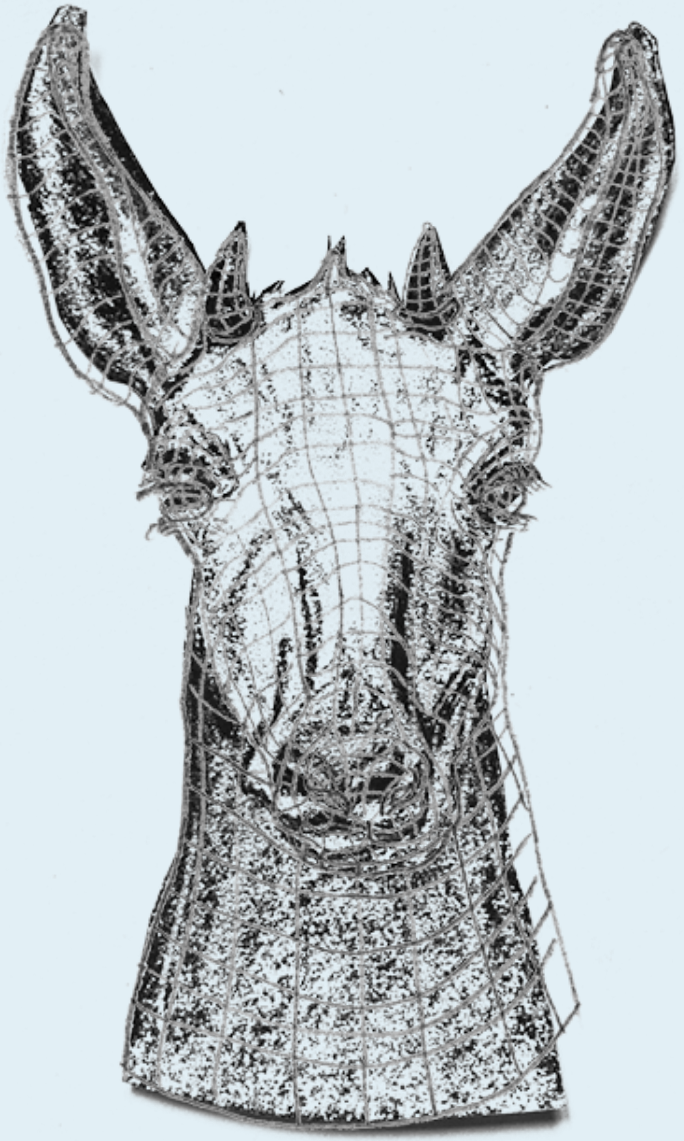
SOMETHING

What does it mean to own

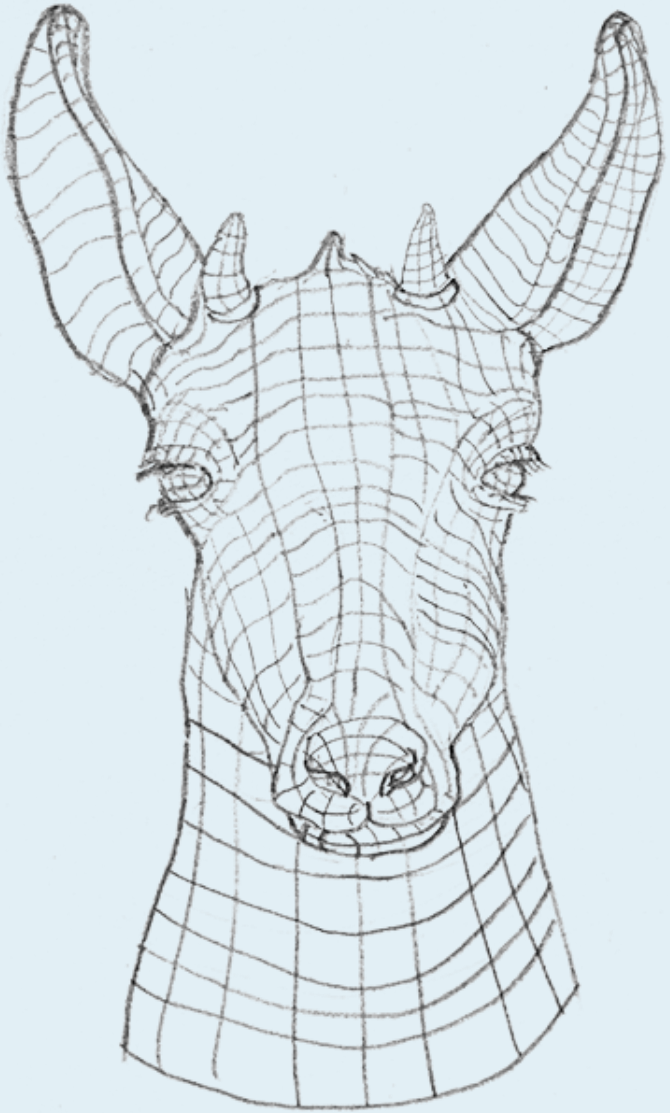
SOMETHING

WHO?
WHEN?
HOW?

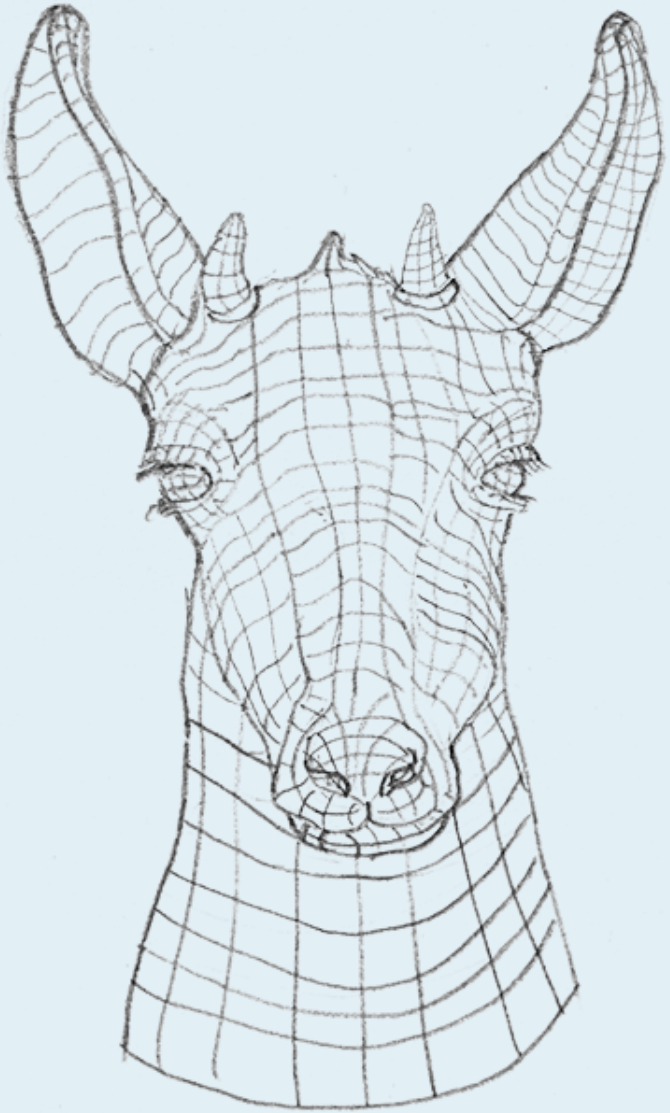





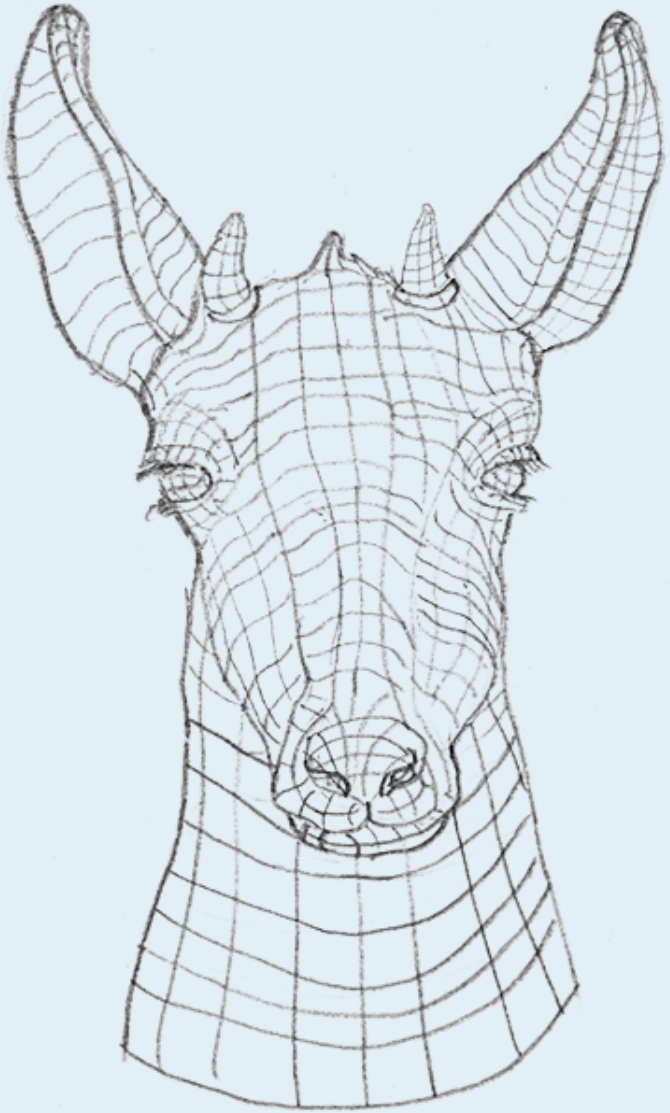
LEGALLY DIGITAL

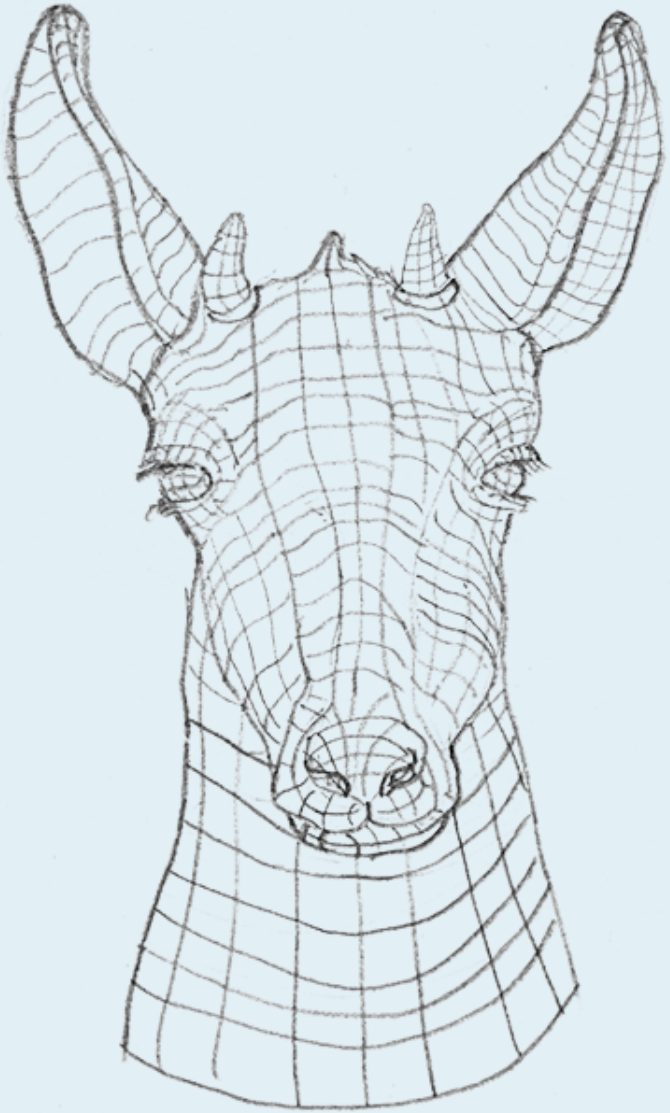


TRUSTED IDENTITY



mobile connect





CONNECT

SERVICES

APPLICATIONS

SERVICES

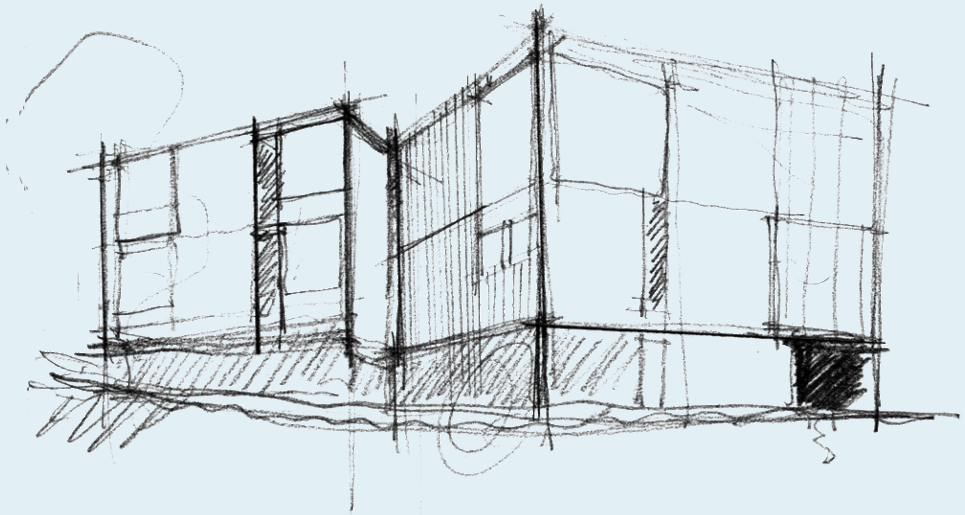
APPLICATIONS

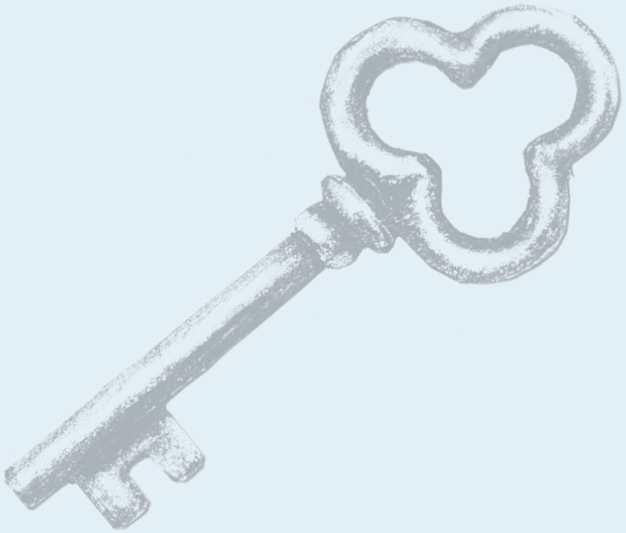
EXPERIENCE

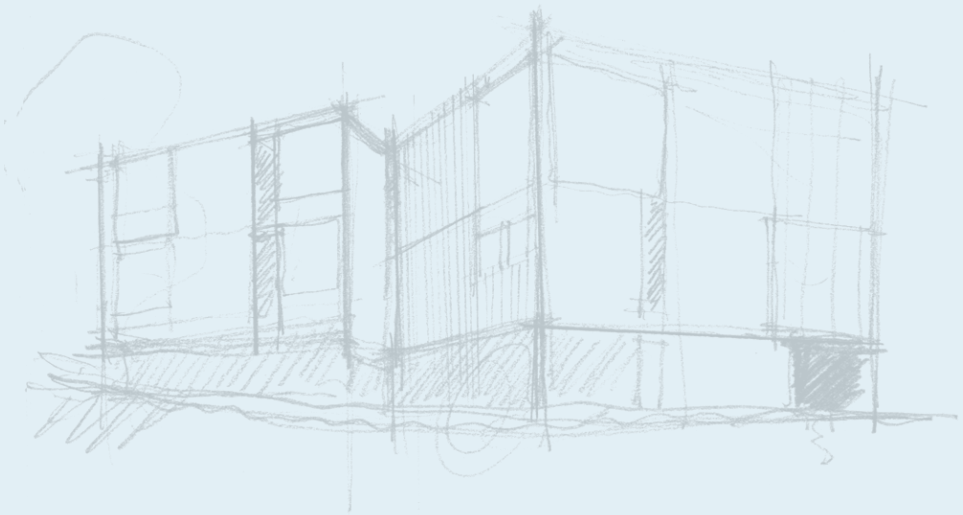
HUMAN

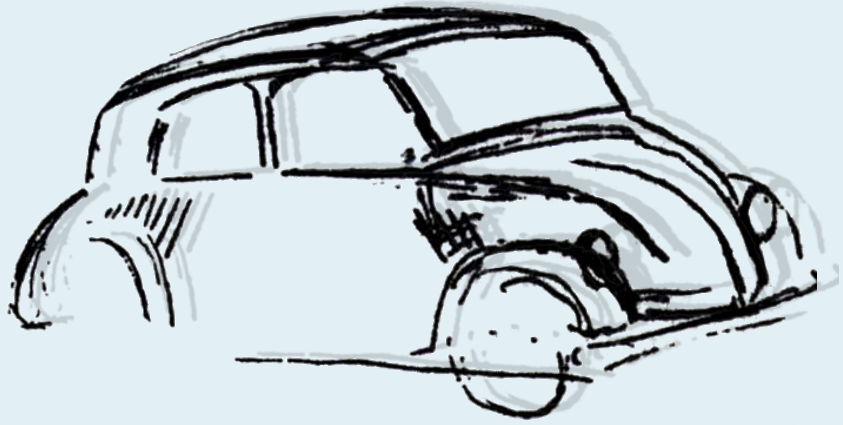
CENTRIC

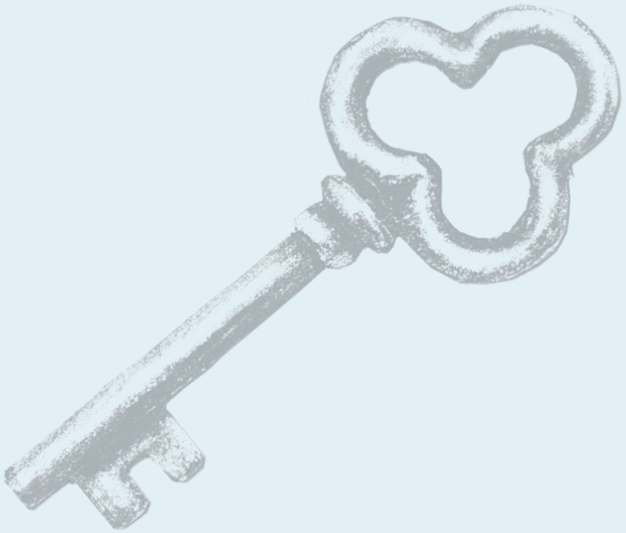
WHO?
WHEN?
HOW?











OPERATORS OF THE FUTURE

REINVENT
CONNECTIVITY

THE FUTURE UX OF AUTHENTICATION

Mobile Connect Summit, Singapore Nov 2017

Markku Mehtälä, VP Authentication

www.insidesecure.com

inside secure
DRIVING TRUST

DISCLAIMER

This presentation and the information it contains are not intended to constitute, and should not be construed as an offer to sell or a solicitation to buy or subscribe to any INSIDE Secure securities, in any jurisdiction. Any public offering of INSIDE Secure securities would be made by means of a prospectus previously approved by the AMF that contains detailed information about INSIDE Secure. The disclosure, distribution and publication of this presentation may be restricted by law in certain jurisdictions and persons into whose possession any document or other information referred to herein comes should inform themselves about and comply with any such restrictions. INSIDE Secure takes no responsibility for any violation of any restrictions by any person.

This presentation contains certain forward-looking statements relating to the business of INSIDE Secure, which shall not be considered per se as historical facts, including the ability to manufacture, market, commercialize and achieve market acceptance for specific projects developed by INSIDE Secure, estimates for future performance and estimates regarding anticipated operating losses, future revenues, capital requirements, needs for additional financing. In addition, even if the actual results or development of INSIDE Secure are consistent with the forward-looking statements contained in this press release, those results or developments of INSIDE Secure may not be indicative of their in the future. In some cases, you can identify forward-looking statements by words such as "could," "should," "may," "expects," "anticipates," "believes," "intends," "estimates," "aims," "targets," or similar words. Although the management of INSIDE Secure believes that these forward-looking statements are reasonably made, they are based largely on the current expectations of INSIDE Secure as of the date of this communication and are subject to a number of known and unknown risks and uncertainties and other factors that may cause actual results, performance or achievements to be materially different from any future results, performance or achievement expressed or implied by these forward-looking statements. In particular, the expectations of INSIDE Secure could be affected by, among other things, uncertainties involved in unexpected regulatory actions or delays related notably to building and operating permits and renewable support policies, competition in general or any other risk and uncertainties developed or identified in any public documents filed by INSIDE Secure with the AMF, included those listed in chapter 4 “Risk factors” of the 2014 “document de reference” approved by the French financial market authority (the Autorité des marchés financiers – the “AMF”) on April 30, 2015 under number R.15-030. In light of these risks and uncertainties, there can be no assurance that the forward-looking statements made in this communication will in fact be realized. Notwithstanding the compliance with article 223-1 of the General Regulation of the AMF (the information disclosed must be “accurate, precise and fairly presented“), INSIDE Secure is providing the information in these materials as of this communication, and disclaims any intention or obligation to publicly update or revise any forward-looking statements, whether as a result of new information, future events, or otherwise.

©Inside Secure 2016. All Rights Reserved. Inside Secure,® Inside Secure logo and combinations thereof, and others are registered ® trademarks or tradenames of Inside Secure or its subsidiaries. Other terms, logos and product names may be trademarks of others.

Inside Secure - trusted by the world's top companies

Banks and payment system	CHASE, Santander, VISA, mastercard
Content distributors	HBO, QUICKPLAY, sky, orange, Virgin media, amazon
Top IT companies	SAMSUNG, htc, ASUS, hp, CISCO
Major semiconductor companies	BROADCOM, QUALCOMM, intel, Texas Instruments, MStar semiconductor

Protecting the solutions of the broadest range of customers: service providers, content distributors, security system integrators, device makers, semiconductor companies

inside secure
DRIVING TRUST

Mobile Connect and UX

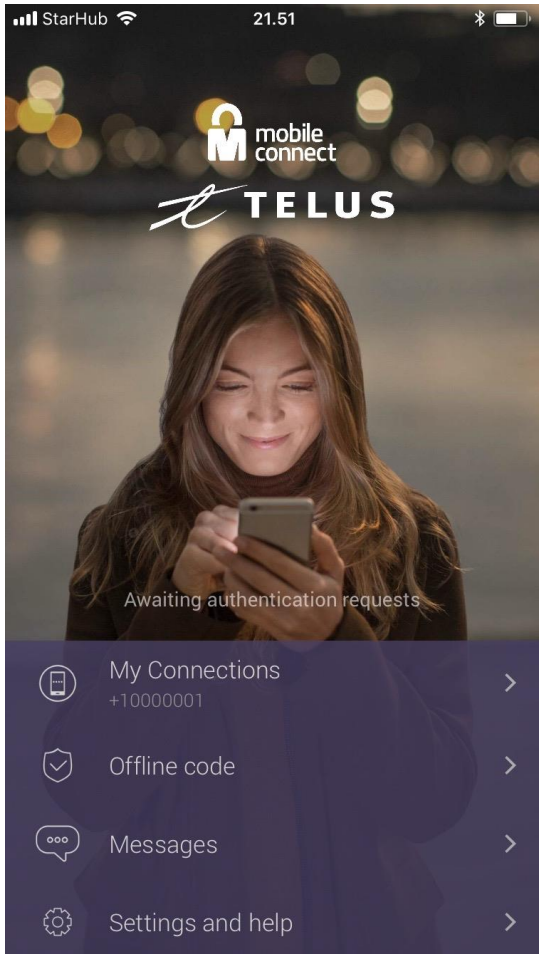
Mobile Connect and UX

Consumers

Service Providers

Mobile Connect and UX

Consumers



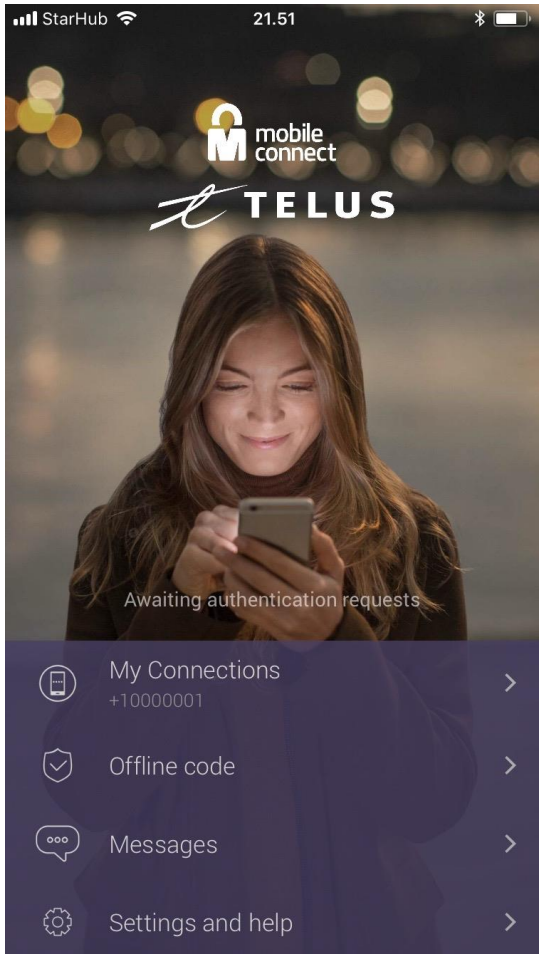
Service Providers

inside secure
DRIVING TRUST

Mobile Connect and UX

Consumers

1) Clarity
2) Service adoption
3) Biometrics
4) Additional utility

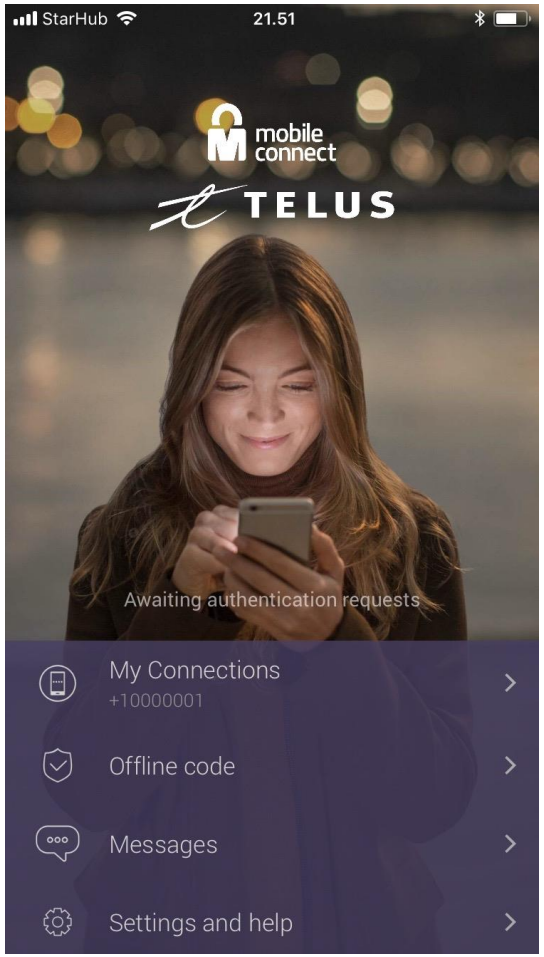


Service Providers

Mobile Connect and UX

Consumers

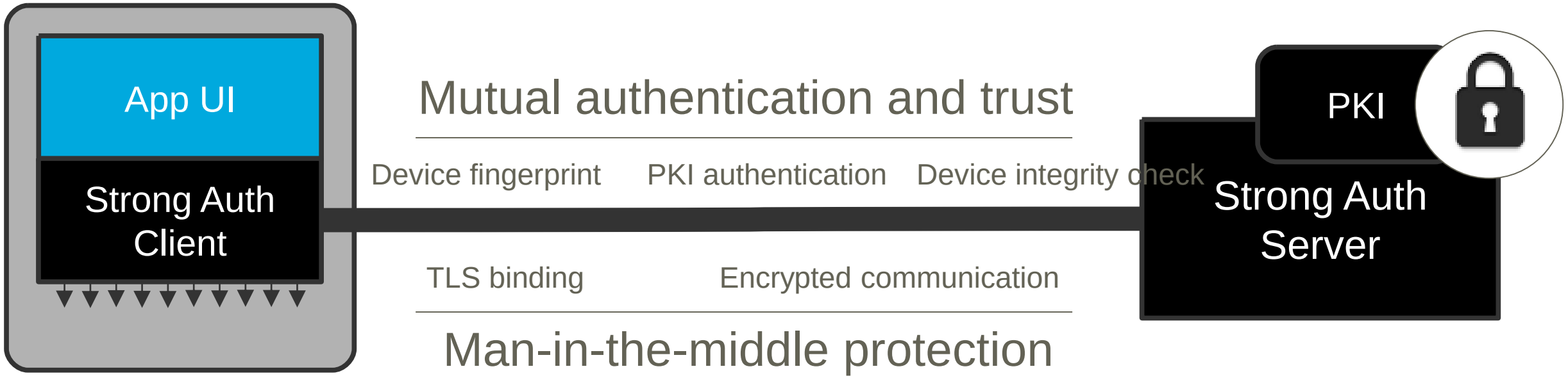
1) Clarity
2) Service adoption
3) Biometrics
4) Additional utility



Service Providers

1) Clarity
2) Consumer adoption
3) Flexibility
4) Additional utility

The future of Authentication UX is already here



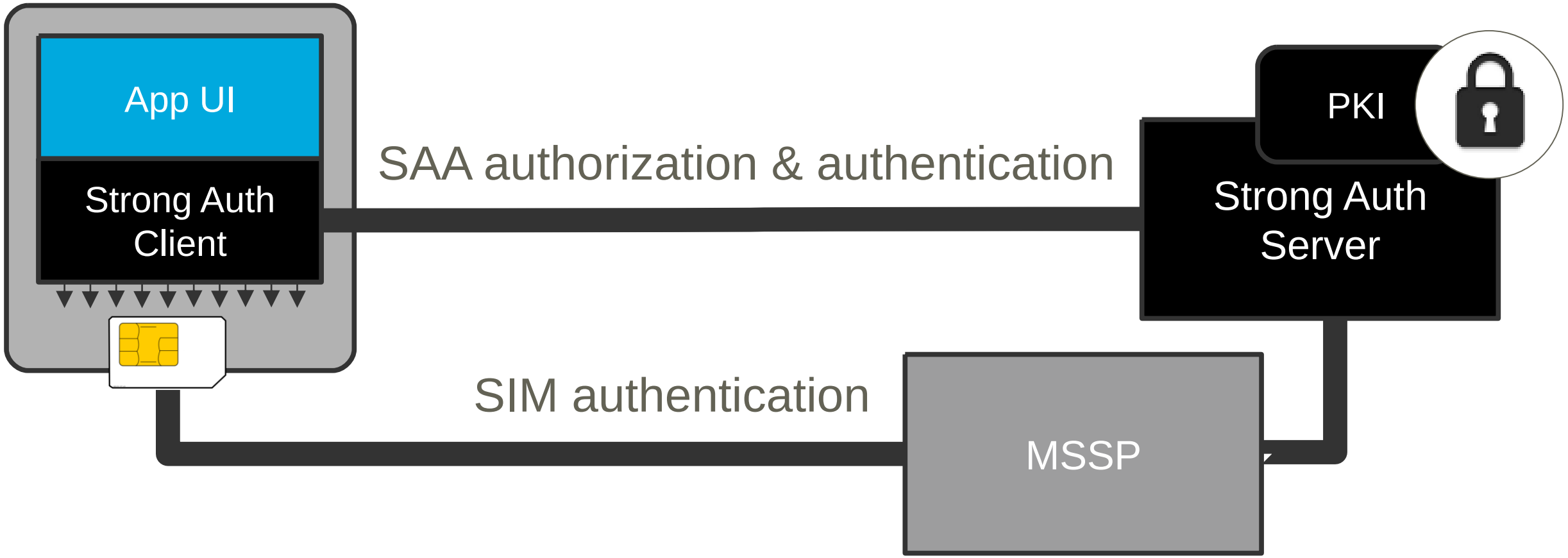
Protection against malware & attacks

OS / platform security
PIN/FP/Face verification
Local data encryption
Device - data binding
Jailbreak/root detection
Whitebox / HW crypto (FIPS certified)
Code obfuscation / tamper detection
Mobile network binding
SIM card binding
(Opt) Trusted Execution Env integration

Device & transaction verification

Device revocation check
Transaction integrity check
Digital signature verification
Collecting additional data for 3rd party fraud detection tools

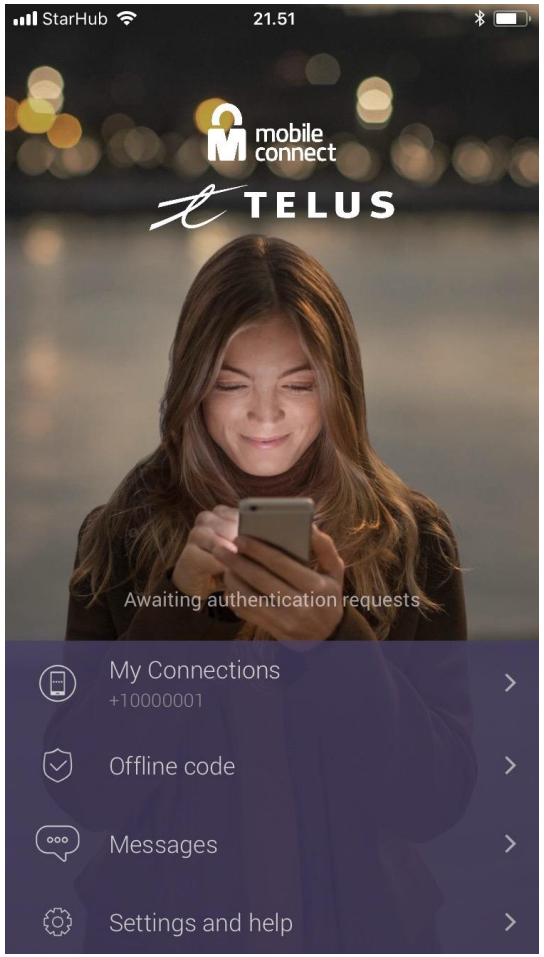
The future of Authentication UX is already here



Additional value and utility to drive adoption and usage

Consumers

1) Service management
2) Trusted messages
3) Payments
4) Device protection



Service Providers

1) User data
2) Trusted messages
3) Payments (online)
4) Payments (contactless)

Add value with UX and Smartphone App Authenticator

THANK YOU

mmehtala@insidesecure.com

inside secure
DRIVING TRUST

Digital ID for KYC based on DLT

ASTRI

2017

香港應用科技研究院有限公司
Hong Kong Applied Science and Technology Research Institute Company Limited

ASTRI: Powered by technology

Founded by the Hong Kong SAR Government

•1046/751 filed/granted under 24 IPC. Tech transfer 673 since 2009.

~500 R&D professionals pursuing innovation and excellence in applied science and technology – Over 28% have PhD and 50% have master degrees.

ASTRI Proprietary

ASTRI Initiatives

Financial Technologies

ASTRI supports the development of FinTech in Hong Kong in three distinct workstreams: Cybersecurity, ...

Intelligent Manufacturing

Intelligent Manufacturing is the development and implementation of artificial intelligence in produc ...

Health Technologies

ASTRI's seeks to guide and facilitate the growth of Hong Kong's healthcare industry and its ecosyste ...

Next Generation Network

ASTRI's Next Generation Network (NGN) Initiative develops new technological infrastructure and platf ...

Smart City

Information and Communication Technology (ICT) facilitates every aspect of the Smart City paradigm. ...

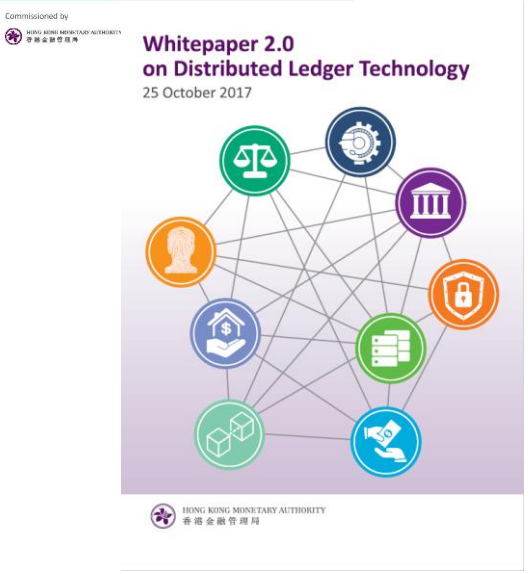
ASTRI Blockchain Technology

White Paper on Distributed Ledger Technology commissioned by HKMA

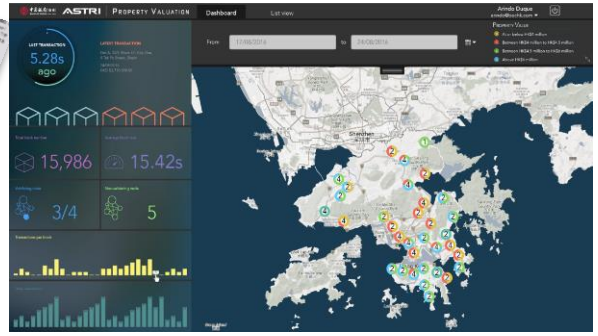
HONG KONG MONETARY AUTHORITY
香港金融管理局

Blockchain POCs:
Property Valuation, Trade Finance, & Digital-ID

Blockchain deployed Applications:
BoCHK, Insurance Start-up



First Production-Grade Property Valuation Blockchain

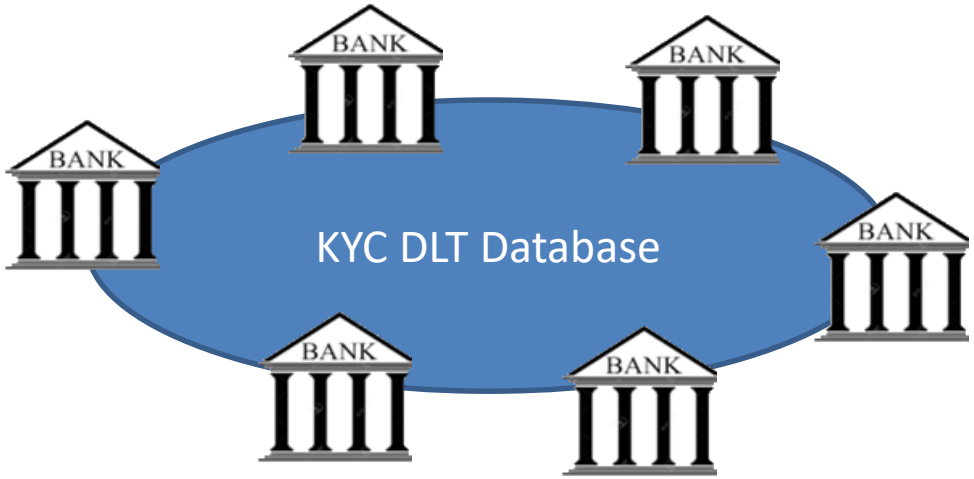


中國銀行(香港)
BANK OF CHINA (HONG KONG)

Digital Identity for Banking: KYC

- For banking regulation compliance
- A process by which banks obtain client information
- Ensures banks' services are not misused
- Completed by the banks while opening accounts
- KYC information is periodically updated

DLT Enabled KYC Information Sharing



Features

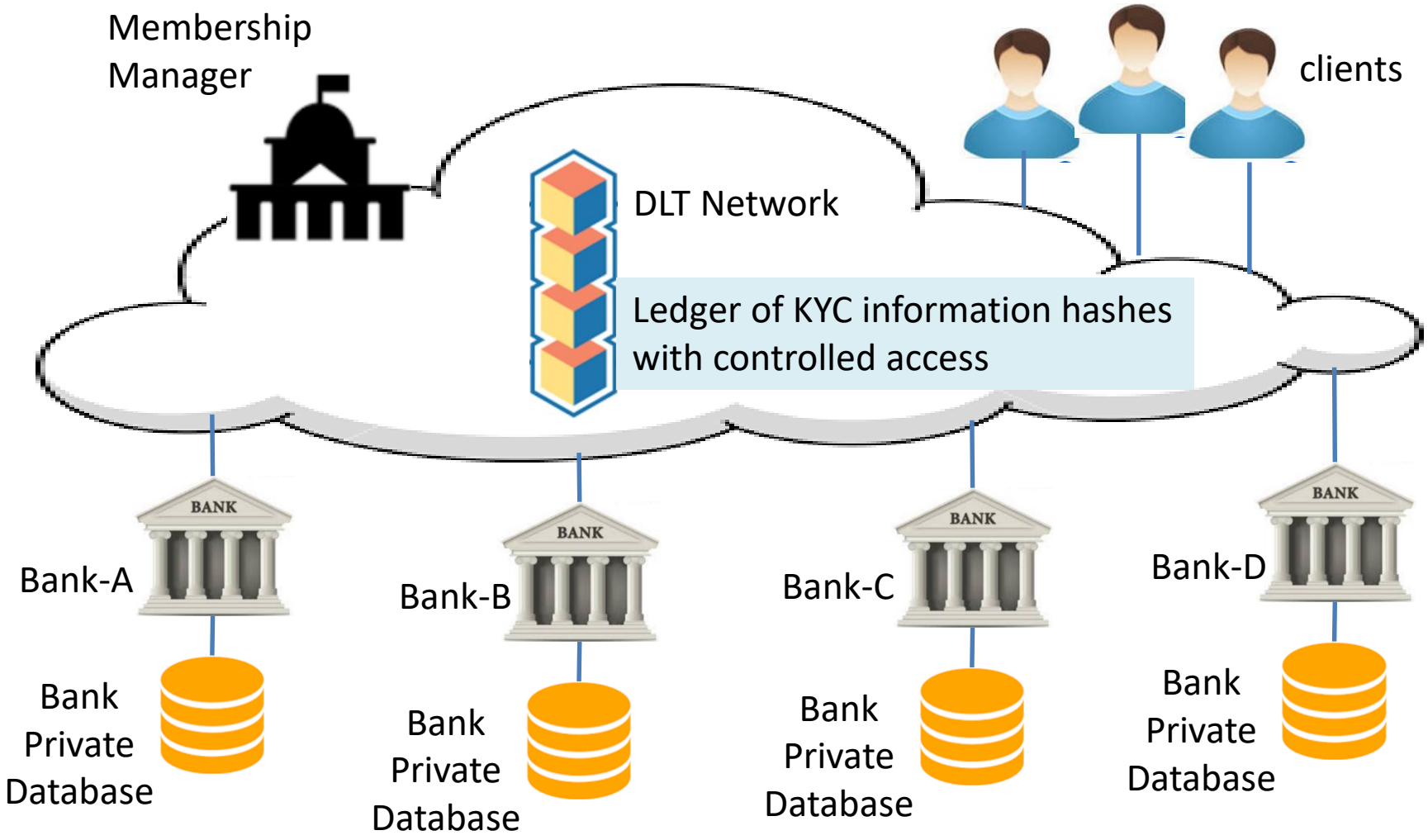
- A DLT system as immutable storage of verified client KYC information
- Banks store verified client information to DLT
- Other banks retrieve verified client information from DLT
- Real time notification to banks about KYC information updates

Benefits

- Simplify client banking experience
  Clients do not need to re-submit information to multiple banks
- Simplify and lower the cost of bank's KYC compliance procedure
  Banks can rely on verified KYC information from other banks

ASTRI Proprietary

PoC Configuration



ASTRI Proprietary

Example Client KYC Information

Information	Data Element of Individual
Identify Information	1. Customer Name in English and Chinese 2. Identification ID (e.g. HKID, Passeport, etc.) 3. Nationality 4. Date of Birth
Employment Information	1. Employment Status 2. Employer's Name 3. Position / Job Title 4. Annual Income
Contact Information	1. Address (Residential & Permanent) 2. Contact Telephone Number (Home & Mobile) 3. Email Address
Digital Document	1. Identity Proof 2. Income Proof 3. Address Proof (e.g. Bank Statement, Electricity Bill, etc.)

Example Client KYC Information Metadata

Metadata

- Bank attached additional information for client Hash entry in DLT
- Added by bank when submitting client KYC information hash to DLT
- Banks may define any metadata

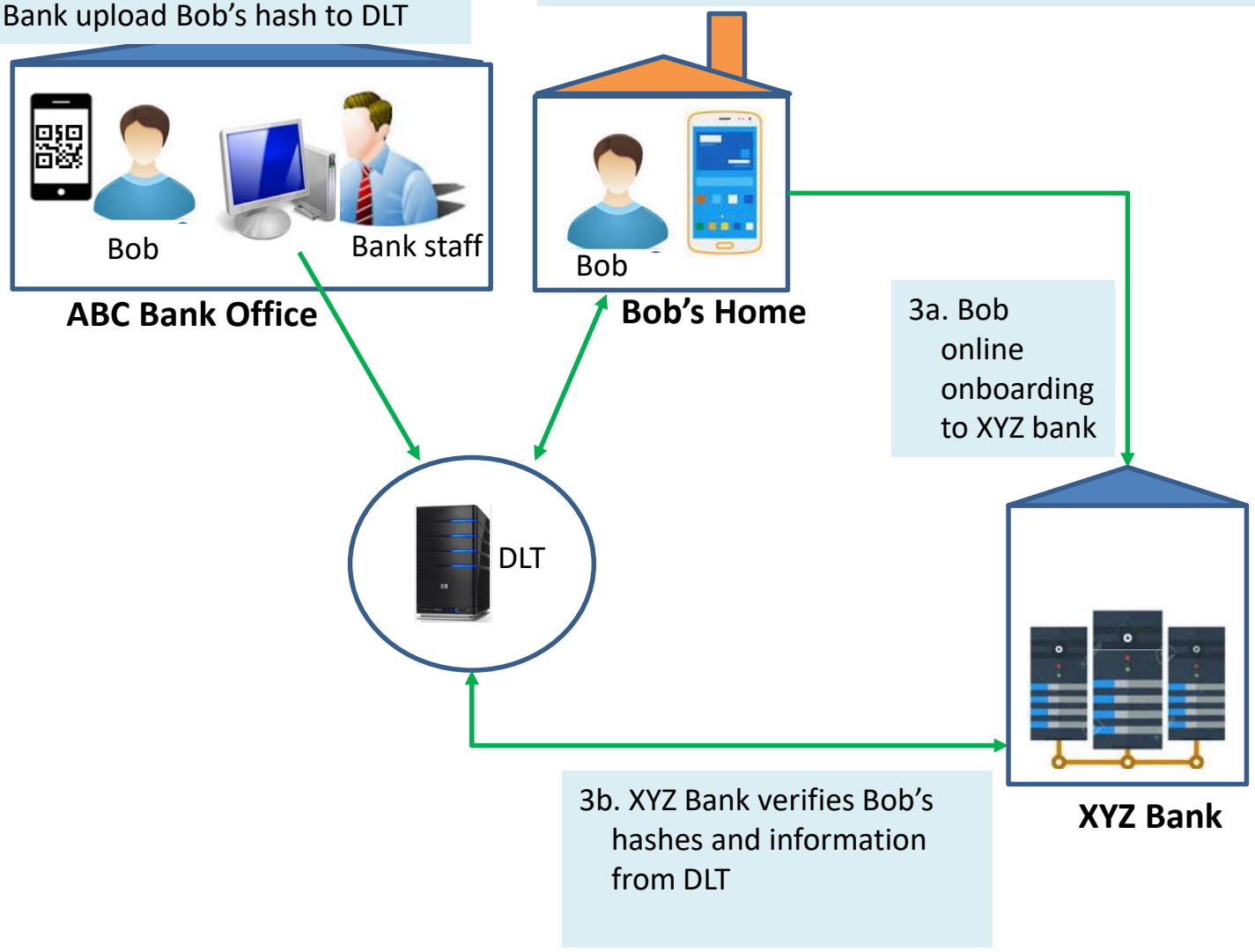
Example of Metadata

Metadata	Data Content
Valid Period	1. Start Date 2. End Date
Bank Comment	1. Text String Example: "*Contact Preference: email*"

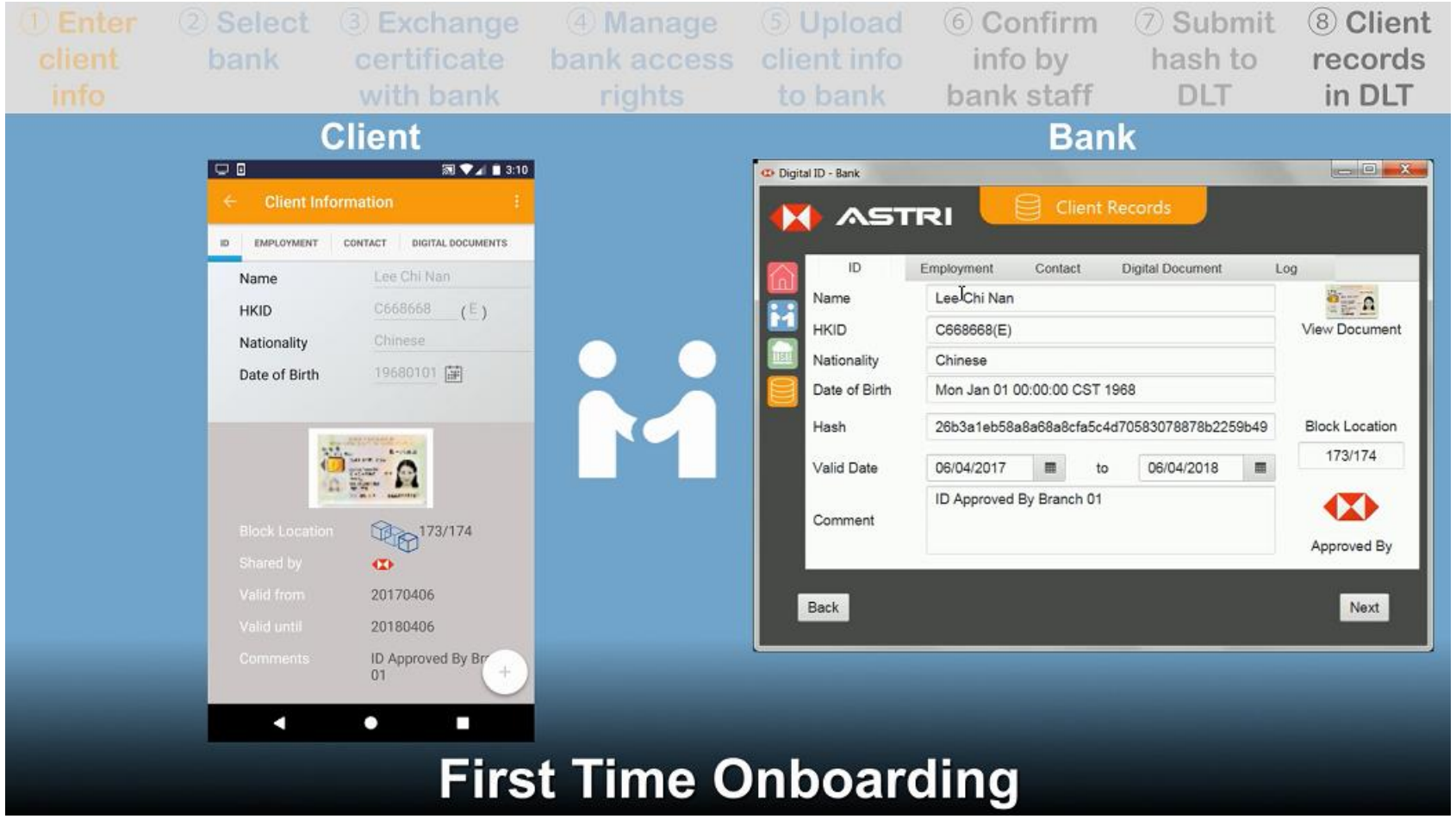
PoC Demonstration

1a. Bob first time onboarding at ABC Bank office
1b. Bank upload Bob's hash to DLT

2a. Bob confirms presence of information hash in DLT
2b. Bob assigns XYZ bank access rights to DLT



PoC Demonstration



- Bank verifies client submitted personal information
- Bank stores hash values of client information to blockchain
- Hash values in blockchain is viewable by client himself and authorized banks

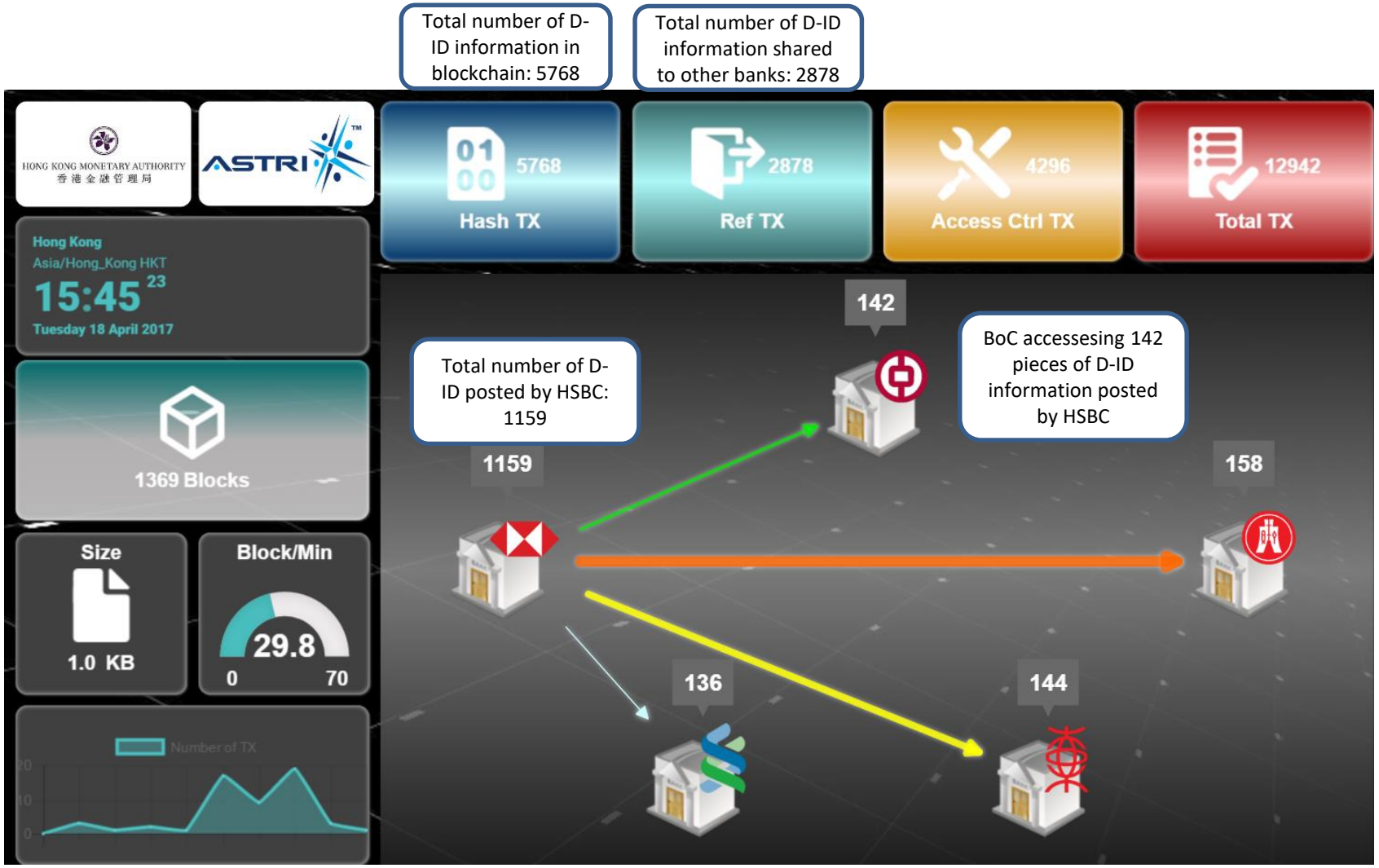
First Time Onboarding

client open account at
bank office first time

Online Onboarding

open another bank account online
after first time onboarding

DLT System Dashboard



Blockchain Statistics

Digltal ID data verification sharing statistics

ASTRI Proprietary

Advantage of DLT D-ID Prototype

- DLT enables interbank synergy
  - KYC information sharing
  - Banks collectively manage DLT system

- DLT enhances reliability and performance scalability
  - each bank owns a copy of KYC database
  - KYC database is replicated
  - redundancy of validating nodes

- DLT system enhances confidence and trustworthiness with:
  - Inter-bank DLT consensus mechanism
  - system transparency
  - KYC immutable records

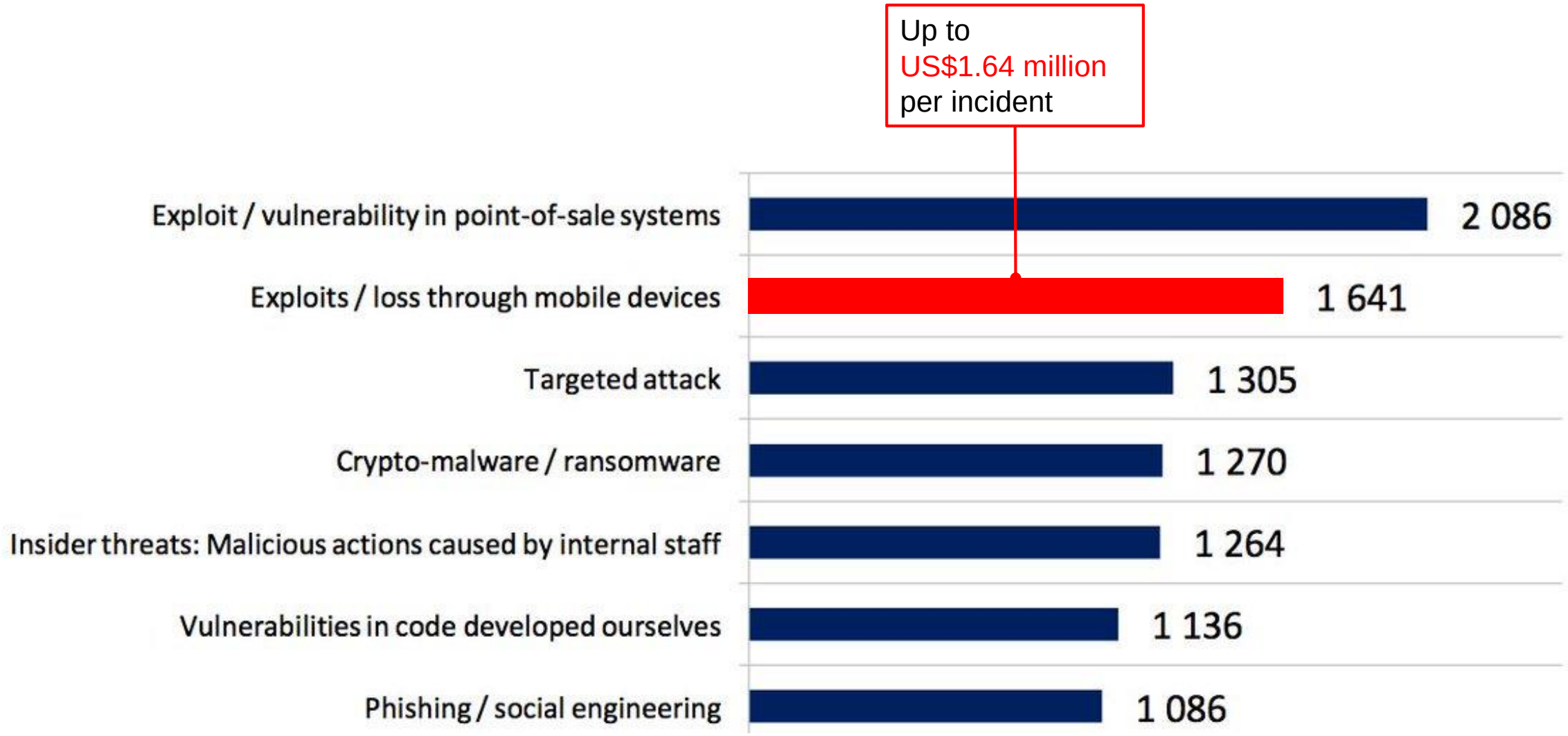
V-KEY
TRUST SIMPLIFIED

TRUSTED IDENTITIES FOR THE NEW DIGITAL ECONOMY

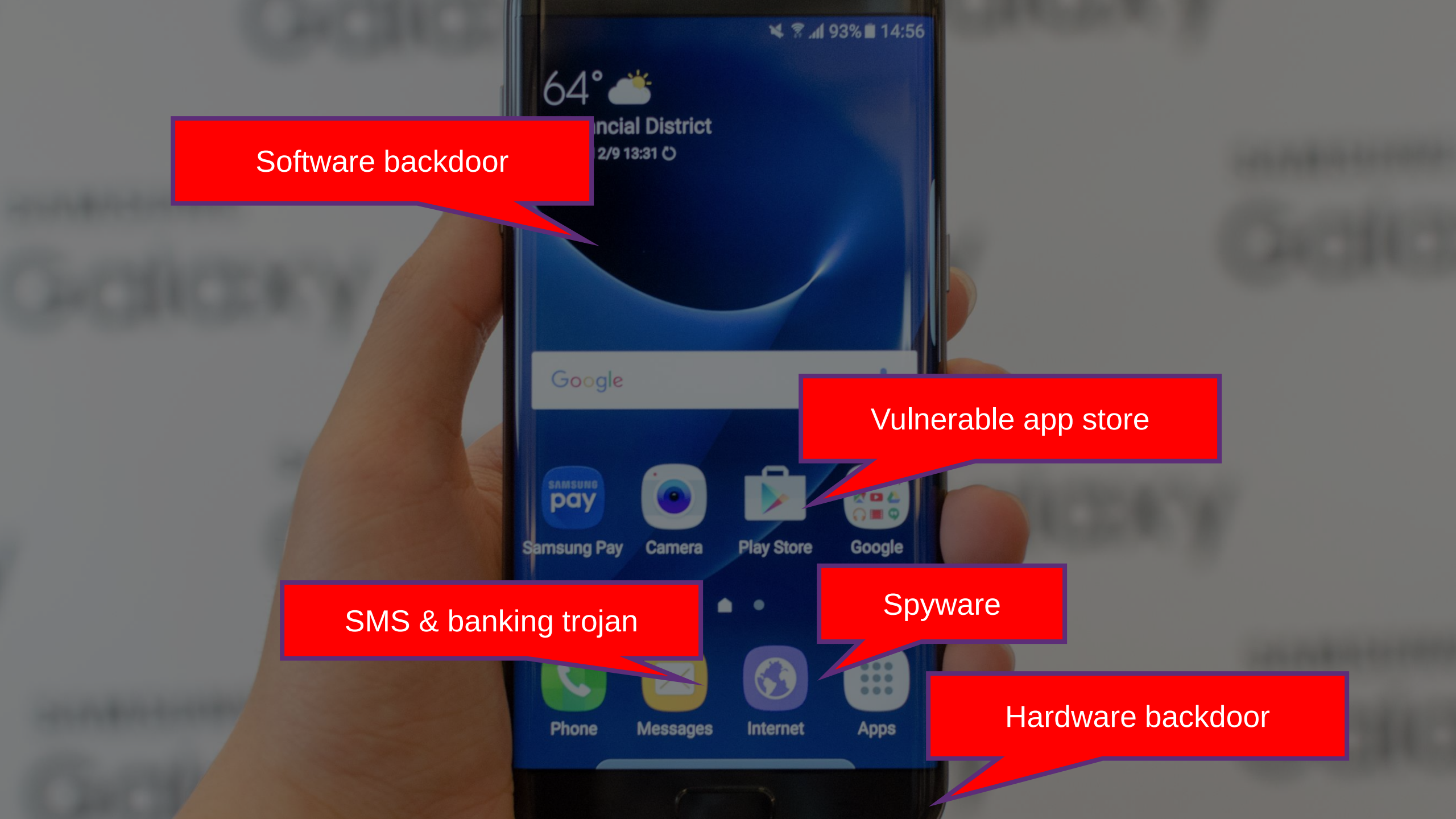
Achieving Ubiquitous Mobile Security

@vkey_inc

The impact of mobile cybercrime



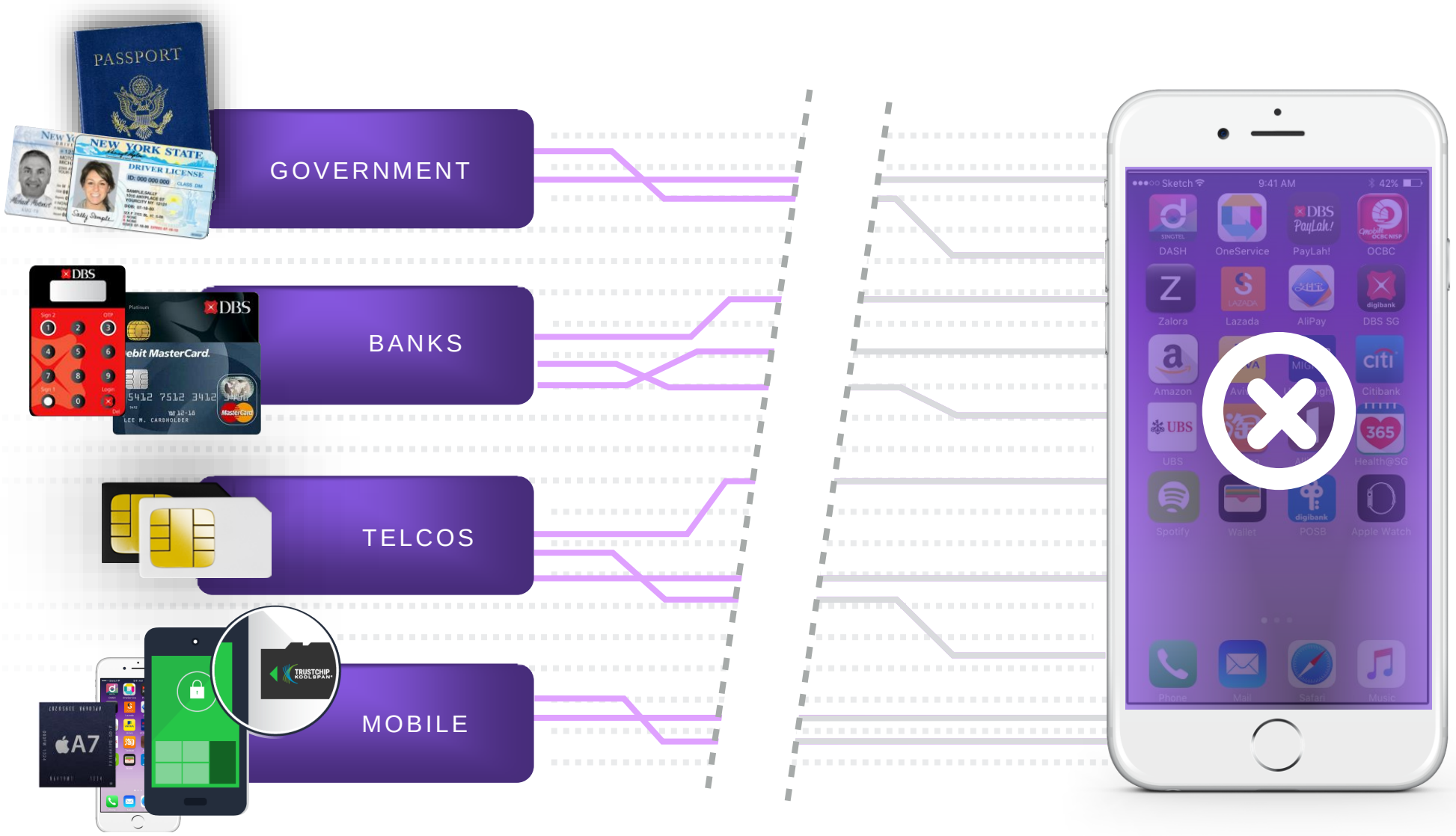
Source: Kaspersky Labs 2017

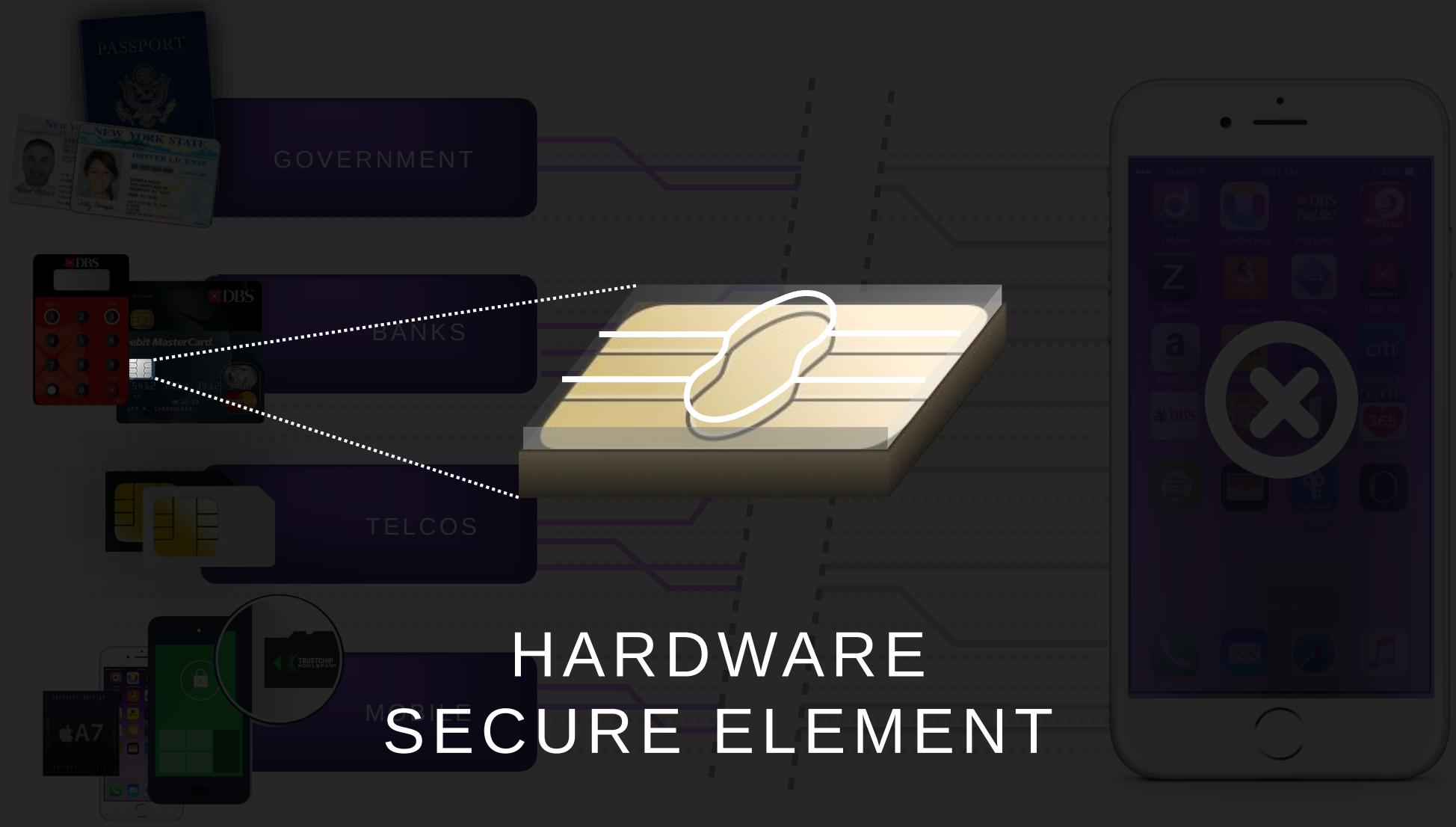

Software backdoor
Vulnerable app store
SMS & banking trojan
Spyware
Hardware backdoor
93% 14:56
64°
Google
Samsung Pay
Camera
Play Store
Google
Phone
Messages
Internet
Apps

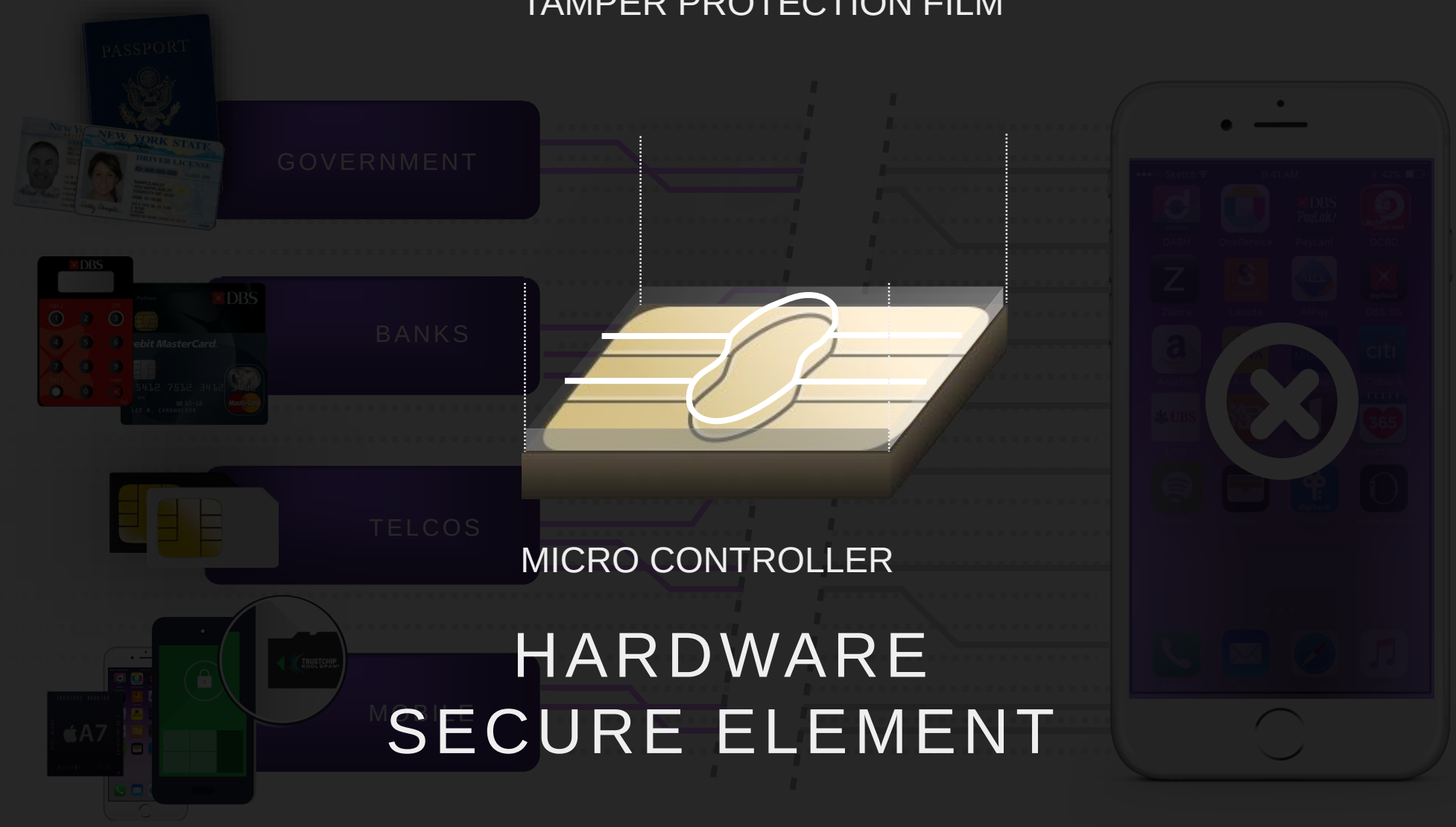
FASTEST GROWING
LEAST SECURE

The global trust ecosystem has been built on the smart card

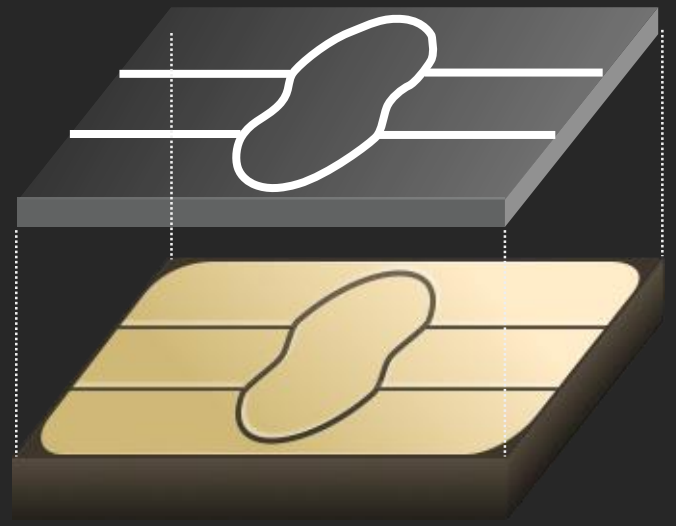
… But there's a LIMIT to how far and fast they can scale




PASSPORT
NEW YORK STATE
DRIVER LICENSE
GOVERNMENT
DBS
BANKS
TELCOS
A7
HARDWARE
SECURE ELEMENT


TAMPER PROTECTION FILM
PASSPORT
NEW YORK STATE
DRIVER LICENSE
GOVERNMENT
DBS
DBS
BANKS
TELCOS
MICRO CONTROLLER
HARDWARE
SECURE ELEMENT
A7

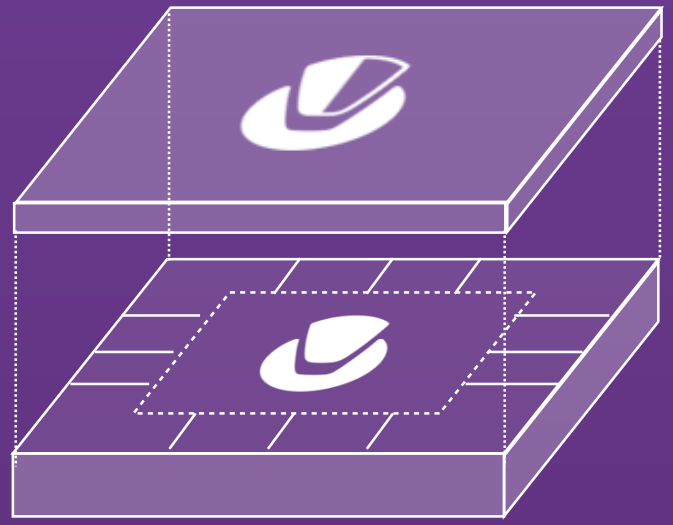
TAMPER PROTECTION FILM



MICRO CONTROLLER

HARDWARE SECURE ELEMENT

TAMPER PROTECTION SYSTEM



CRYPTOGRAPHIC VIRTUAL MACHINE

VIRTUAL SECURE ELEMENT

Built to global standards and certifications

FIPS LEVEL 1 VALIDATED 140-2

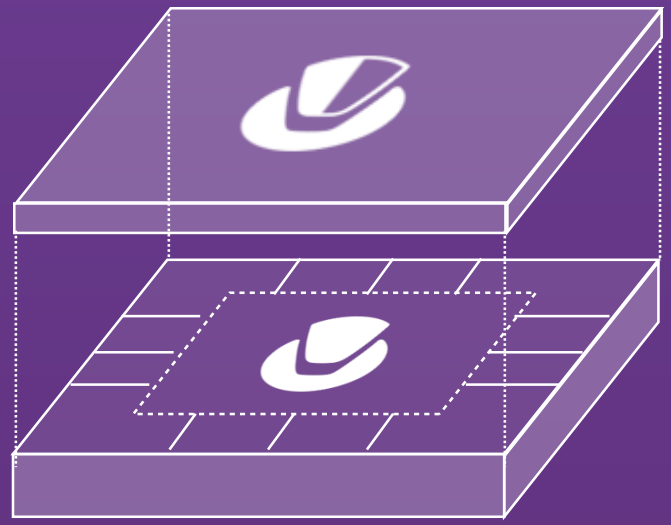
fido alliance member

IM Accredited

GLOBALPLATFORM®

V-OS

PATENTED SINCE 2011



VIRTUAL SECURE ELEMENT

Proven resiliency in multiple global penetration tests

CORE SECURITY

UL

MWR INFOSECURITY

quarkslab TRUST IN INTUITIVE SECURITY

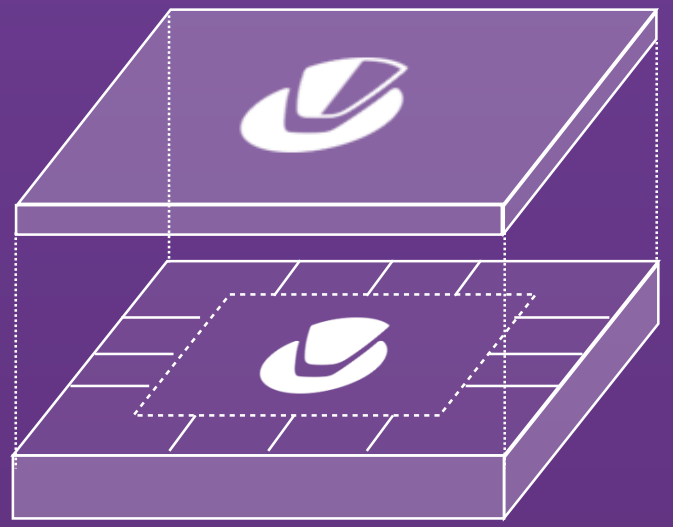
乌云众测

VANTAGEPOINT

Deloitte.

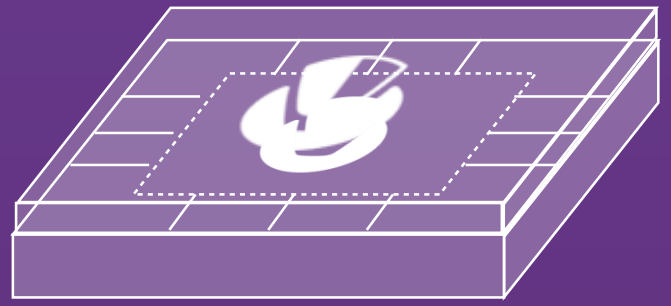
RESOLVO

@vkey_inc



HOW IT'S USED

V-OS is embedded within an iOS or Android mobile app.



SECURING CRITICAL DATA & PROCESSING

UNTRUSTED OS

SECURE APP

Tamper protection system

Root of Trust

Secure Digitized Use Cases

Secure Digitized Use Cases

Mobile Identity

OTP/PKI Token

Secure Messaging

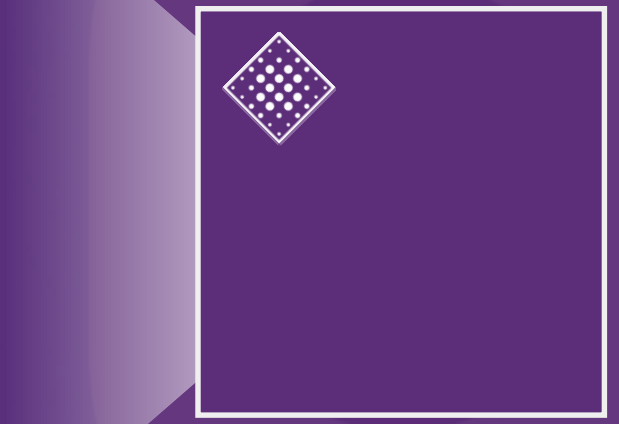
Mobile Biometrics

Application Protection

Seamless Authentication

Document Signing

Electronic KYC



@vkey_inc

V-OS Management Center

Mobile Identity

OTP/PKI Token

Secure Messaging

Mobile Biometrics

Application Protection

Seamless Authentication

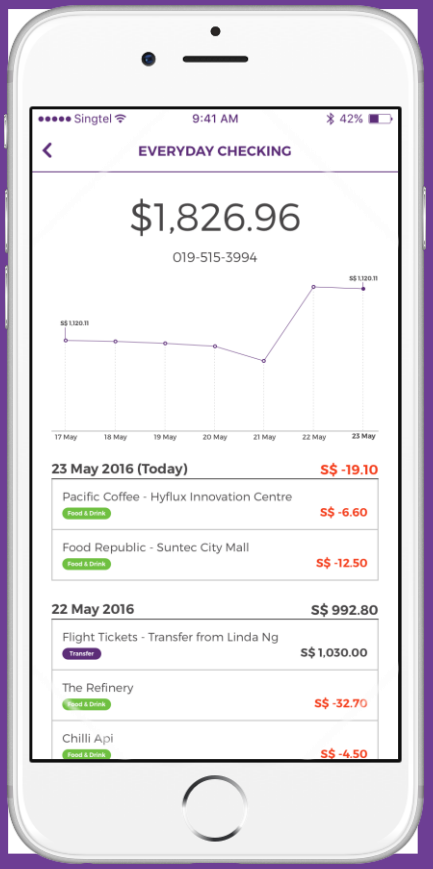
Document Signing

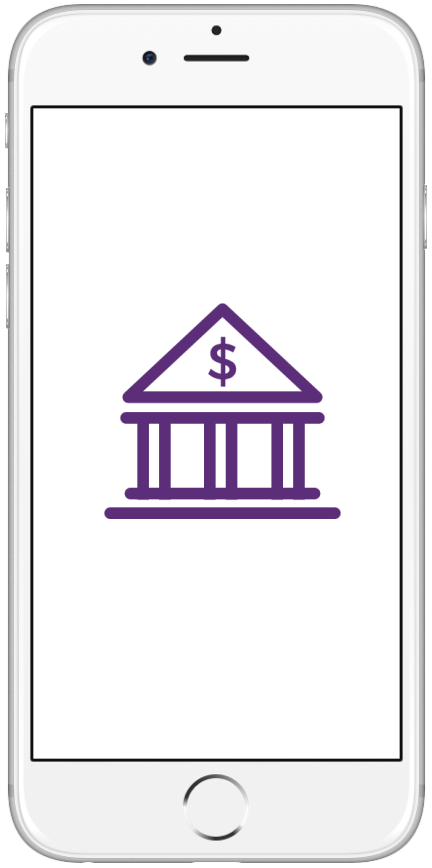
Electronic KYC

V-OS Virtual Secure Element

V-OS Trust Platform

@vkey_inc


Singtel
9:41 AM
42%
EVERYDAY CHECKING
$1,826.96
019-515-3994
17 May
18 May
19 May
20 May
21 May
22 May
23 May
23 May 2016 (Today)
S$ -19.10
Pacific Coffee - Hyflux Innovation Centre
Food & Drink
S$ -6.60
Food Republic - Suntec City Mall
Food & Drink
S$ -12.50
22 May 2016
S$ 992.80
Flight Tickets - Transfer from Linda Ng
Transfer
S$ 1,030.00
The Refinery
Food & Drink
S$ -32.70
Chilli Api
Food & Drink
S$ -4.50



US$10
Replacements

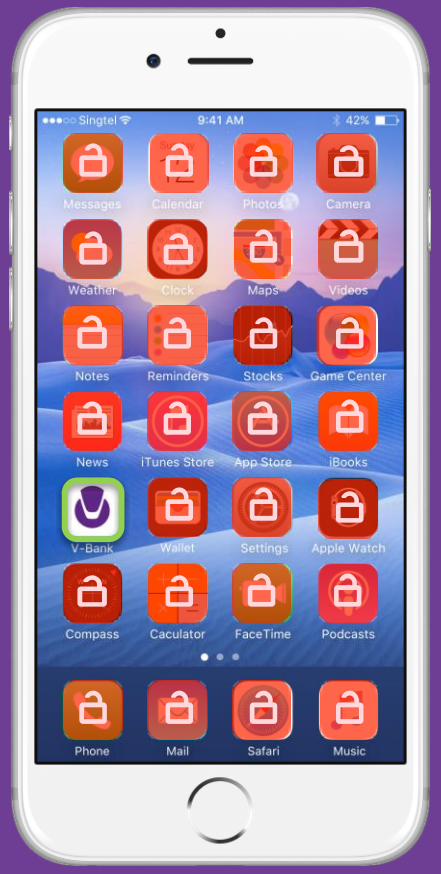
Inconvenient

Dynamic

Scalable

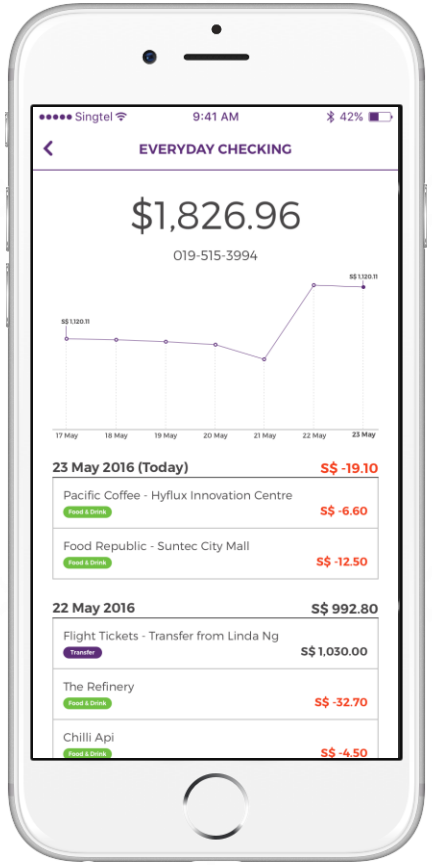
Safer

Convenient

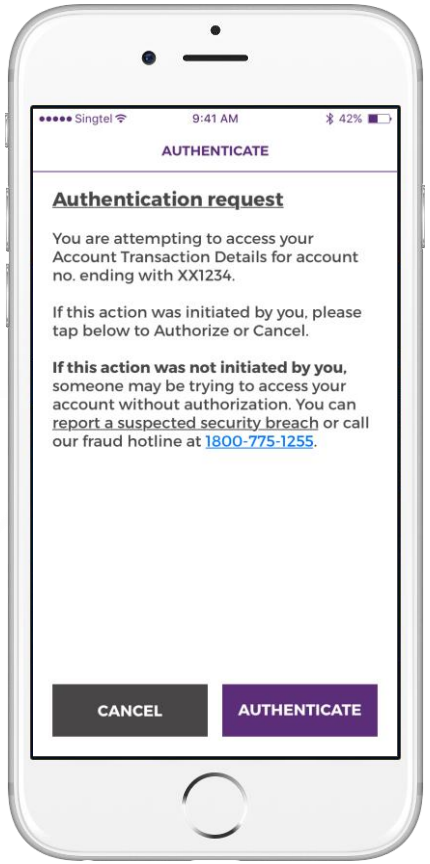


V-OS Authentication

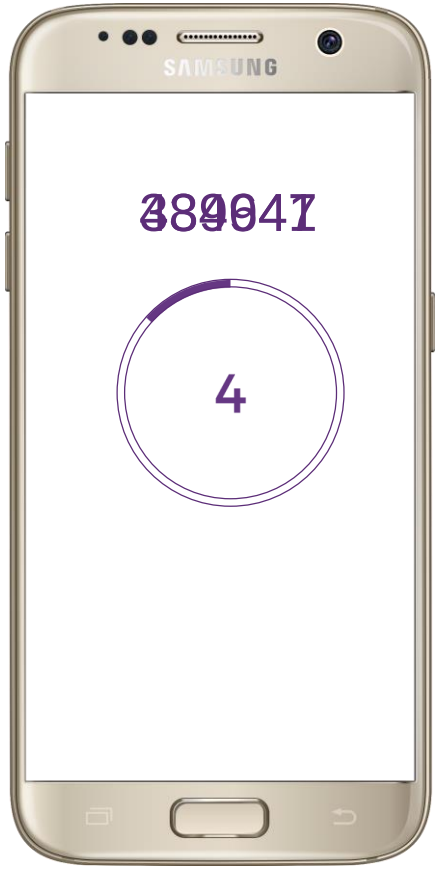
Replacing hardware tokens and SMS OTPs



SEAMLESS AUTHENTICATION



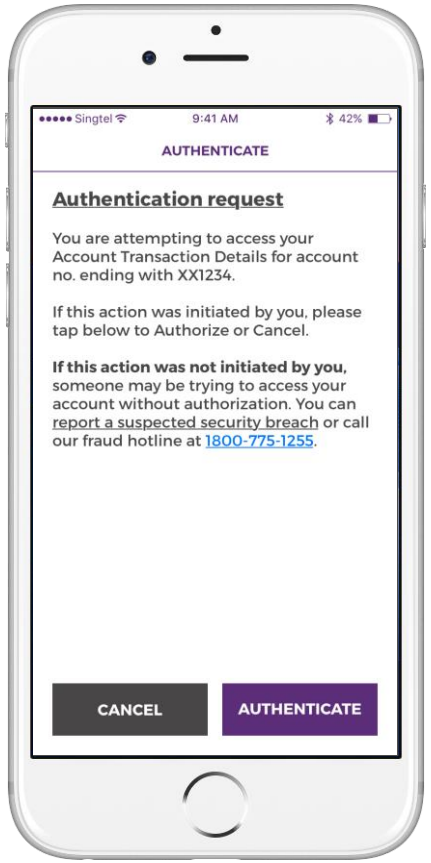
SECURE MESSAGING



OTP TOKEN

Mobile Connect: V-Key Secure Message Service

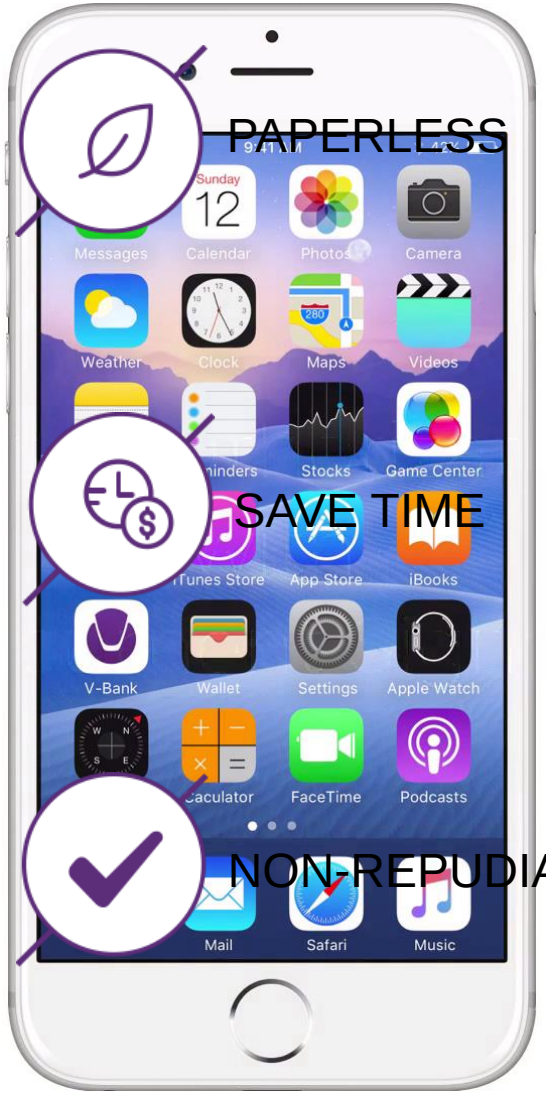
Supporting high-risk transactions and sensitive notifications



- Authenticate with a single tap
- Out-of-band authentication
- Secured Software PKI Technology

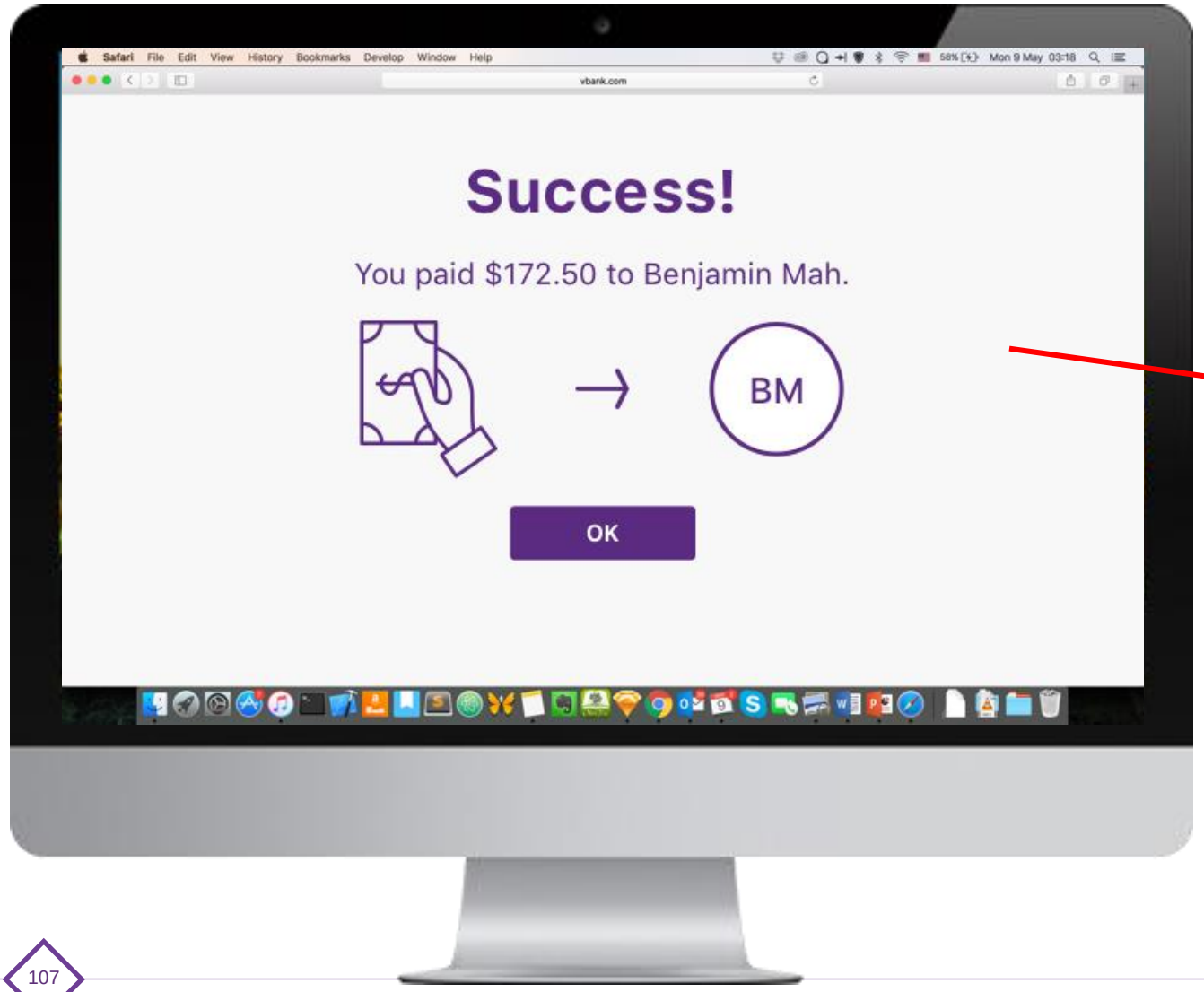
Mobile Connect: V-Key Secure Message Service

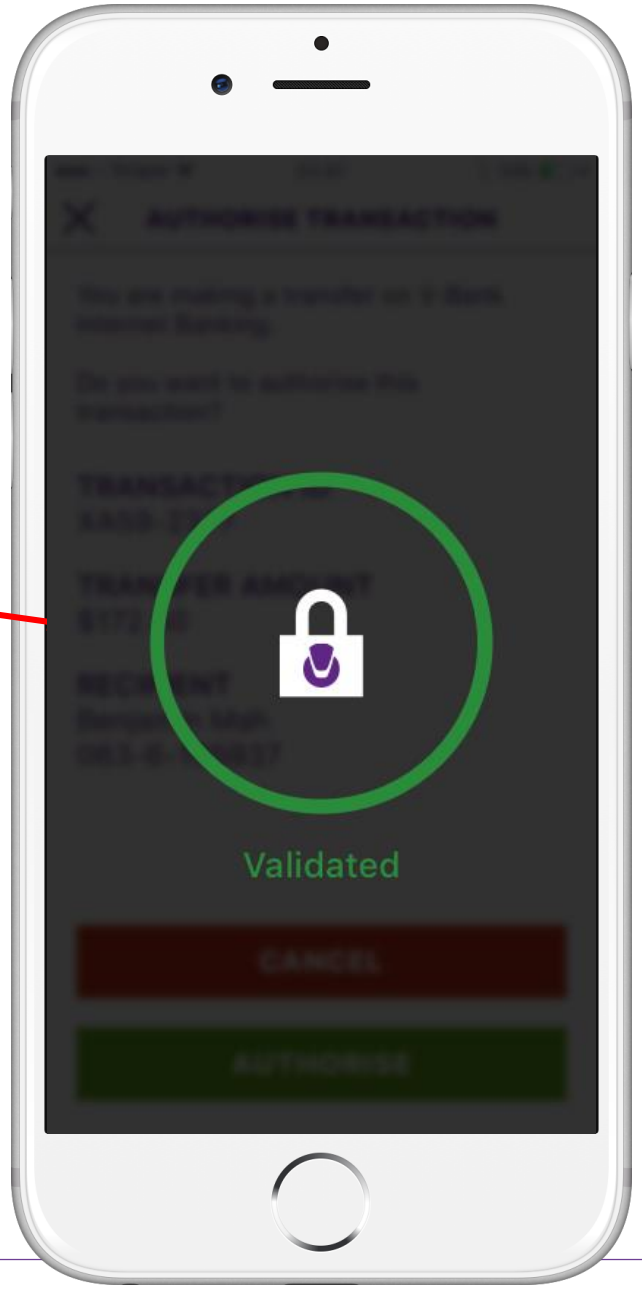
Mobile Authorization



Secure Message Service

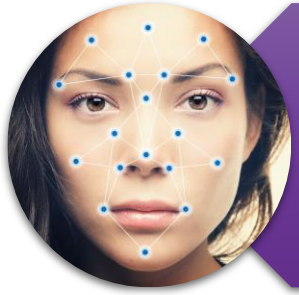
Authorizing Omni-Channels





National Digital Identities: Beyond Authentication

Authentication & Authorisation



Biometric eKYC On-Boarding

Digital Signatures

App-to-App Transactions

Mobile Payments

Federated Identity

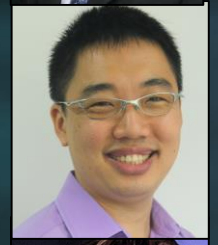
Thank You

For any enquiries, please contact us at enquiries@v-key.com

@vkey_inc

Emerging technology trends in identity services, and the part they play in the consumer need for convenience vs security

Venura Mendis, CEO, WSO2 Telco



Mr Joseph Gan, President and CEO, V-Key

Rikard Strid, Founder, Clayster

Markku Mehtälä, Founder and CEO, MePIN / Inside Secure

Moderator

Jaikishan Rajaraman
Global Head of Technology
GSMA

#MCSxSG

#MCSxSG