Mobile Operators and Fintech

April 2017

Security Classification: Non confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

1 Introduction

Mobile Operators and fintech companies are obviously very different entities: different industries, different sizes, different cultures. But there are strong reasons for them to join hands in bringing innovative and secure solutions to market *at scale*, *because* they are so different - or should we say, complementary: fintechs bring rapid innovation and flexibility ; operators provide a powerful access to market with their marketing and distribution capabilities, as well as some specific enablers, available at scale, that facilitate their partners deployments. As a matter of fact, operators already join forces with small, innovative companies to deliver differentiating services to their customers – not necessarily in the finance area. But, in this paper, we will see that opportunities to build value are particularly interesting with fintech companies. We will review what operators can provide them and why it makes sense for both parties. Then we will take the opposite angle, going through some existing or soon-to-be fintech services and showing how they can benefit from operators' capabilities. Note that a very specific case is that of mobile operators moving into financial services – typically becoming banks, or mobile money providers in emerging markets.

2 Why should fintech partner with operators?

2.1 Find scale

This is the most obvious part of the operators' value proposition to partners – fintech or other, let's call them "service providers". Operators provide powerful marketing and distribution channels, that can include :

- Promotion and download through the operator's online channels or apps
- Other specific promotion activities
- Pre-load of partner application on handsets distributed by the operator
- Co-branding
- First level of customer support.

Obviously some of these assets are only used with parsimony for specific partners, but the principle is always that the operator brings exposure to market and, in return, can provide their customers with enhanced access to differentiating services. The business model varies :

- The operator is a pure distributor (and possibly an enabler as well, see below) : the service provider pays the operator, typically through revenue share. In practice the operator can collect the money for the service provider, e.g. via carrier billing.
- Co-branding: the operator usually sells the service and pays the service provider accordingly.
- Operator service : the service provider is an enabler and is paid like a supplier, usually per customer or per event.

We'll keep this section short because, although it's an important source of value for partners, it's not specific to fintech. Of course, there will be more opportunities for fintech companies with operators who themselves move into financial services : beyond the opportunistic distribution and

marketing deal, there can be more strategic synergies between each player's services, leading to a more compelling compound value proposition to consumers. But the sheer distribution capacity of operators is in itself a major business accelerator for any innovative service provider. Such an accelerator indeed, that two traps need to be avoided :

- think that the distribution pipe is infinite : operators need to be selective as they cannot afford to spam their customers. Service providers should not be frustrated by this, it is unavoidable.

- in case of a successful partnership, the scale comes suddenly, even brutally for a small service provider, who should make sure their infrastructure and cash flow can hold the tide.

2.2 Leverage useful enablers : Mobile Connect

The most common example of operator enabler is carrier billing, that dramatically improves the conversion rate of digital contents purchase – simply because the customer can pay seamlessly without the hassle (and worry) of entering payment credentials. But in this section, we will focus on a new enabler that transforms the customer experience while bringing massive value to partners – with specific use cases that are particularly relevant for financial services. This enabler is called Mobile Connect.

2.2.1 Mobile Connect in a nutshell

Mobile Connect is a cross-operator mobile identity framework that supports the following services :

- user authentication via their mobile phone, using the mobile phone number as the primary user identifier. The user selects "login via Mobile Connect" on the service provider's login page and is prompted by their operator to authenticate, e.g. by tapping to confirm the ownership of their mobile phone ("something you have"), and also, if a second factor is needed, by entering a PIN/Personal Code ("something you know") (the same PIN/Personal Code is used across different service providers) Or even biometrics like fingerprints, iris scan or facial biometrics (“something you are”). Different levels of assurance are supported depending on the service provider's requirements. The authentication service can also be “passive” or “adaptive”, where the confidence in the authentication can be enhanced by contextual information about the user known by the network like SIM status, device used, network presence etc. (“something the network knows”).

- user data sharing or matching, also called identity and attributes services: with the user's consent, Mobile Connect allows the service provider to access data or check it against their own. This can be demographics data like name, address, age etc associated to a given phone number, network data like network presence, location, SIM status or account status.

- authorisation : the user is presented a text issued by the service provider (and possibly additional information provided by the operator) and is asked to confirm their agreement, typically to confirm a transaction. Here again, the service offers different levels of assurance.

From the service provider's perspective, registering to the global Mobile Connect framework (managed by the GSMA) and using the relevant SDK gives transparent access to all the operators supporting the service, which jointly represent over 3 billion users across the world today. Not all

of them support the whole Mobile Connect portfolio of services, but capabilities are being deployed at pace.

2.2.2 Some interesting use cases

Simplify sign up

Sign up form filling is a major hurdle of customer enrolment, with high drop-out rates. Mobile Connect allows users to pre-fill their forms with data held by their operators, using Mobile Connect Attribute service. Alternatively, the service provider can check the data provided by the user against that held by the operator, e.g. to improve their KYC[1] process.

Simplify sign-in (can be combined with the above)

This is the basic Mobile Connect authentication service, with a variable number of authentication factors (e.g;. phone ownership +PIN) and various levels of assurance. It solves the user's "password nightmare" (a single PIN to remember) whilst improving security.

Simplify check-out

Mobile Connect can simplify check-out at two levels:

1. Pre-fill checkout forms with name, shipping address, invoicing address, possibly payment details (e.g. card details or bank account details), depending on available attributes.
2. Collect user consent for payment through Mobile Connect authorization service.

Facilitate KYC

Mobile Connect allows KYC checks : Anti-Money Laundering rules require financial institutions to verify their customers' "real" identities on a regular basis. To do so, they need to check the data they have (e.g. name, surname, address). Based on the phone number, they can check it against the data held by their customers' operators.

But operators and fintech can also work together on more innovative approaches to KYC, saving significant costs and hassle to service providers and consumers :

- how to perform KYC remotely, at least for some services
- how to make a KYC process reusable by other parties (aka transferable KYC).

Antifraud-account protection

Some e-merchants and financial institutions monitor user and transaction data to detect fraud patterns. The more data they have, the more accurate their fraud detection engines, allowing them to give more freedom to their customers – i.e. less hassle though re-authentication. With their customer's consent, mobile operators can share relevant user data with these service providers to improve their fraud detection engines. Examples of such data can be recent SIM swap, recent change of phone, country check (is the phone associated to the customer's number in the country where a transaction is taking place) etc. Alternatively, operators can provide an aggregated risk rating.

Another use case consists in checking that the user actually "owns" the phone number they have provided to their service provider, and is using a device attached to this phone number. A typical

[1] Know Your Customer, customer identity checks mandated by regulation for some financial services.

example consists in making sure that a user is installing a banking app on a phone attached to the phone number held in the bank's records.

Facilitate payment initiation

First of all, payment initiation requires user authentication. Mobile Connect authentication service can be leveraged to this end, as briefly described above. But another innovative use case can be supported: an increasing number of payment services are using the mobile phone number as a primary account identifier, after linking it to a payment account. The payment order then takes the following form : "send £XX from phone #YY to phone #ZZ". Using the phone's address book, this approach can radically simplify the user experience. Mobile Connect can enable such services by :

- resolving the phone number/account number mapping with a simple attribute service : the attributes are the payer's and payee's payment account details attached to their phone numbers. The Mobile Connect framework makes this natively interoperable across all the operators that support these attributes.
- authenticating payers and collecting their consent.

Note that the underlying payment method can vary : Direct Carrier Billing, e-money transfers, Card on File payments, virtual cards hosted in digital wallets, bank transfers (for bank transfers, see also section 2.2.3 below).

2.2.3 In Europe: PSD2 specifics

Payment Services Directive 2 (PSD2) has passed into European law and is in the process of being rolled out into state laws. The directive builds on its predecessor (PSD) and is designed to ease payment processes across the European Community, increase competition and encourage innovation. A major feature of the directive is that it requires the banks to open their systems through APIs allowing licensed third parties to initiate transfers or access account information on behalf of account holders. These third parties are regulated but do not have to comply with the capital structure required from actual banks – hence the new roles introduced by PSD2: Payments Initiation Service Providers (PISP) and Account Information Service Providers (AISP). PSD2 also includes specific requirements regarding user authentication that the European Banking Authority is currently standardising - Mobile Connect has all the characteristics to be compliant to these requirements.

In this context, bank transfers are likely to flourish via the APIs exposed by the banks. New PISPs and AISPs will seek of offer secure and easy-to-use services : Mobile Connect's ability to offer simple and secure authentication, and to retrieve payment account details based on phone numbers (in particular for post paid customers who have already provided their account details to their operators), can prove very valuable.

2.2.4 Security considerations

Mobile Connect provides interesting security features that do not require to hassle the end user :

- The use of “something I have”, i.e. a mobile phone, as the primary authentication factor means Mobile Connect is less vulnerable to a scalable compromise/attack than approaches solely based on “something I know” such as password.

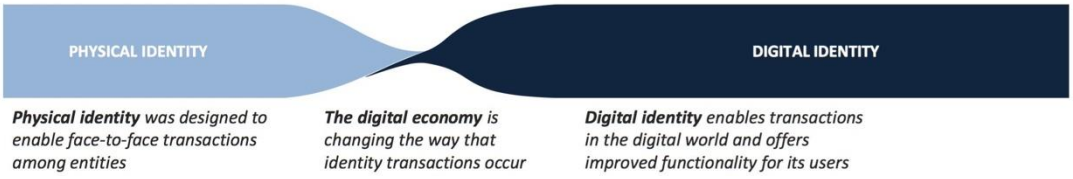
- The Mobile Connect authentication system employs private and secure mobile network operator channels rather than the public Internet, which protects it from man-in-the-middle attacks
- Out of band authentication: the consumer is authenticated via a different channel to the one through which they are consuming the service. For Europe, note that this is one of the PSD2 requirements.
- As mentioned before, Mobile Connect can support secure multi-factor authentication and authorisation, providing an appropriate level of assurance (LoA) authenticator, including multi-layer encryption, in line, for example, with the requirements of the EU Payment Services Directive.
- Mobile Connect requires the service provider and the application to be registered in advance, and authenticates it at each authentication or attribute request. This approach adds an extra layer of security.
- Exchanges between operators and service providers are encrypted as per OpenID protocol specifications.
- The mechanisms described above for the anti-fraud use case can be used to enhance the security of any service.
- "Privacy-by-design" approach is used, so that user is in control of any personal data and only used for matching or shared with user's consent and authorisation
- Mobile Connect is offered by an established player (a mobile operator), with an accessible customer care : this gives extra assurance to consumers.

3 Examples of fintech services that could benefit from partnering with operators

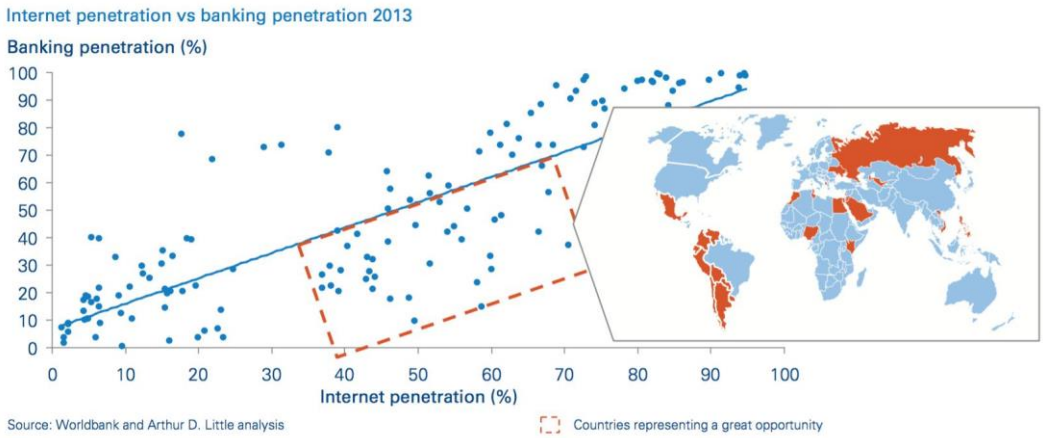
[This section presents a fintech industry perspective; it has been provided by Nicolas Steiner, representative of FINTECH Circle, in collaboration with Level39 and StartupHome]

Identity is currently a critical issue for FinTech innovators. In a world that is increasingly governed by digital transactions and data, several issues need to be addressed:

- Methods for managing security and privacy need to evolve, as data breaches, identity theft and large-scale fraud are becoming more common.
- A significant proportion of the world's population lacks the necessary digital credentials to fully participate in the digital economy.
- Physical Know Your Customer processes hinder the emergence of pure digital offerings designed by FinTech innovators. This positions the development of new generation of digital identity systems as a crucial component to innovation and delivering secure digital-based services.



Besides, in emerging economies, mobile penetration is considerably higher than banking penetration, which provides telecoms with an edge for marketing financial products to their clients through greater reach. As a result, the relation between banking and telecommunication will become increasingly dynamic and complex.



Identity and authenticated user data is the foundation to improve core financial processes and open up new opportunities, especially in the developing world. In such areas, many people are unable to participate in the financial ecosystem as they do not hold any legal or physical identification documents. Therefore, many startups are also looking for innovative ways to cater for this segment of the global population.

Finally, the Blockchain technology, often associated to payments, is also perceived as having the potential to change way identity lifecycle is managed. Therefore the examples below also include some Blockchain based companies.

In that context, we selected the following use cases - showing the link with the enabling capabilities described in section 2.2. Note that these examples are illustrative, and do not constitute an endorsement of the mentioned companies.

Social Lender

Social Lender is a lending solution based on social reputation on the mobile channel, online and social media platforms (primarily Facebook, Twitter and LinkedIn accounts). Social Lender is designed to bridge the gap of immediate fund access for people with limited access to formal credit.

Social Lender uses a proprietary algorithm to perform a social audit of the user on social media, online and other related platforms and gives a Social Reputation Score to each user. The more accurate information provided by the user, the higher the social reputation score. Data sets including basic user details (name, age, date of birth), school and work details, telephone number verification and bank account details enable and enhance the identification process. Loans are guaranteed by the user's social profile and network, allowing users to then borrow from banks and other financial institutions based on their social reputation – completed by the data sets mentioned above.

Tala:

Tala is a mobile technology and data science company that is working on innovative credit scoring methods and financial services. Based in Santa Monica, CA, Tala emerged as a company providing micro-loans in Kenya, Tanzania and the Philippines. Their mission is to bring financial access, choice, and control to underserved people.

Anyone with a smartphone can apply for credit through the Tala app, which evaluates a customer's risk and capacity using only the data on their devices. More than 10,000 mobile data points go into Talas underwriting models, helping them score even those without formal credit or banking history. The app gives Tala access to a range of data, from basic biographical information to the number of people loan applicants contact on a daily basis. Tala can see the size of the applicant's network and support system. The data also reveals where the applicant goes during the day, whether they demonstrate consistency, like making a daily call to their parents, and whether they pay her bills on time. Once approved, a borrower can receive money via their smartphone within minutes.

Creative science

We question everything. We find insights where others don't, analyzing everything from geolocation trends to network diversity to build our algorithms.

Disruptive finance

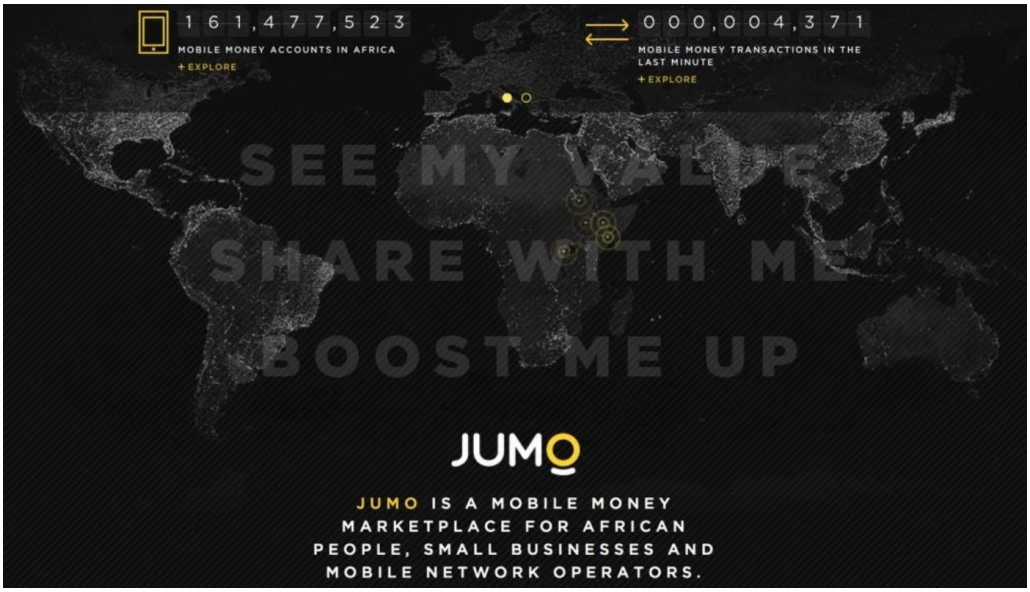
Traditional credit doesn't work in emerging markets — mobile does. On our mobile platform, customers can access credit and other financial services instantly.

Global impact

Our data models have empowered hundreds of thousands of customers globally to choose their financial futures.

JUMO

Based in Cape Town, Jumo partners with mobile operators in countries like Kenya, Tanzania and Zambia, to acquire data on phone usage. Its algorithms analyse a person's smart-phone usage, according to criteria such as: how much they spend on airtime and how they use their mobile money wallet - to come up with a "Jumo score", which is in effect a measure of creditworthiness, thereby creating financial identities for small, medium and micro-sized enterprises (SMME's).



The examples above show the benefits of digitally identifying an individual or a business : it provides the gateway to the financial system, where banks and other stakeholders compete to provide the best savings product or working capital to enhance growth prospects. Furthermore, this method is beneficial for Fintech innovators who wish to deliver digital services without demanding physical forms of identity. This is an innovative way of targeting lower income segments, especially in Africa where a lot of people are unbanked and earn informally.

Blockchain-related examples

Blockchain, or Distributed Ledger Technology (DLT), is a technology protocol that allows data to be shared directly between entities in a network, without intermediaries. DLT has certain key features that hold potential for identity systems:

- Distributed ledgers eliminate the need for intermediaries and therefore lower the cost of completing transactions.
- Transaction history is maintained and verified through the network, preventing the falsification of information.
- Record-keeping and transactions can be executed from any device, both online and offline.

International remittances…

As the volume of international remittances grows[2], drawn by the diaspora of people in search of better paid jobs, more and more mobile money wallets become in a position to receive such remittances, complementing the classical over-the-counter reception. International remittances remain quite expensive and the industry is looking for cheaper channels. Several innovative players are investigating the potential of blockchain to reduce the compliance costs, providing an elegant solution to enable secure transaction recording and monitoring, in particular for anti-money laundering purposes.

… and beyond!

As smartphones become increasingly omnipresent, social media has begun to play a larger role in enabling these types of financial transactions by leveraging digital asset such as authentication delegation API. In late 2016, both Viber and WeChat announced partnerships with Western Union that allow US users to send money to non-US beneficiaries.

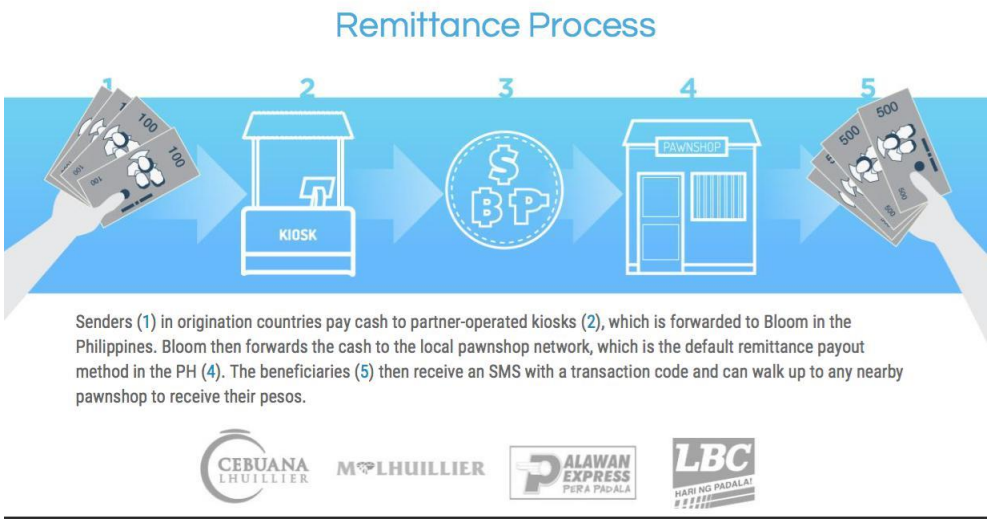
Below is a Blockchain-based remittance service that could use Mobile Connect to consolidate their authentication mechanism and to leverage the mobile operators' distribution channels.

Bloom

[2] Worldwide, 250 million people send $585 billion in remittances each year.

Bloom Solutions, based in Manila, leveraged the Blockchain and developed a mobile wallet that seeks to bring useful features of the modern internet to the most basic phones: search, information services, and also reception of money transfers – all through simple SMS commands. With Blockchain, Boom seeks to disrupt the cross-country payment fee charges by

classic industry players, then to leverage the foundation for micro-financial services by developing Digital Identity services (see also below).



A final use case of collaboration between Mobile operators and the blockchain technology is related to Digital Identity LifeCycle.

In this context, Mobile Connect provides user authentication and manages the access to user identity data by third parties, while Blockchain technology providing the ledger and provisioning aspects of an identity solution – i.e. guaranties the validity of the user identity data.

In other words, Mobile Connect acts as the authentication solution, manages the user's wallet and enables on-boarding into additional services, while the blockchain solution is the trusted record-holder that "proves" the identity, therefore leveraging the mobile channel to link the user to value-added, financial, or social services.

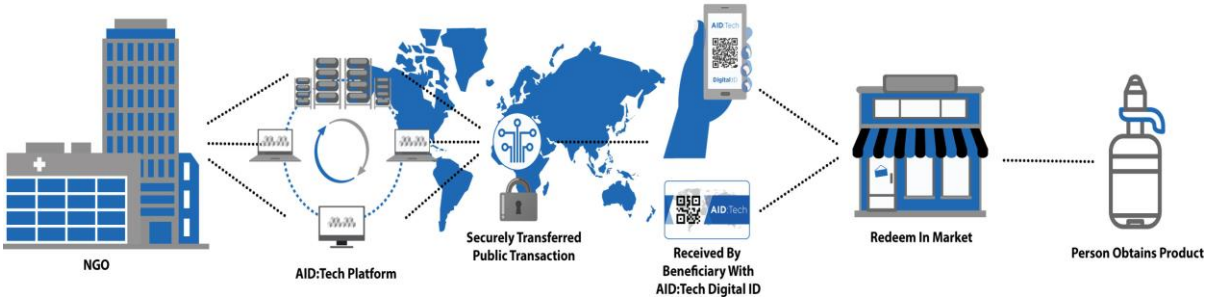
Here are a couple of examples :

AID:Tech

AID:Tech has built a platform based on blockchain technology in order to provide a transparent recording system that allows individuals with no formal proof of identity to gain access to the social, education and financial systems.

Their mission is to bring their technology solution to both emerging and developed markets, to help the estimated 2.4 billion people worldwide that are unidentified to join, or re-join, the social and economic system.

Here is an overview of the AID:Tech solution works (blockchain is used to securely record the transactions):



With AID:Tech's blockchain based platform, organisations can transparently send funds and services to an individual anywhere in the world in real-time: beneficiaries are issued with a Digital Identity which allows them to be uniquely identified. Using this unique identifier, funds and services can be received completely transparently with a permanent immutable record stored on the blockchain. The graphic above shows an example where an NGO sends a digital asset representing a bottle of water to a beneficiary. The beneficiary then uses their AID:Tech Digital Identity to redeem against a bottle of water obtained in a shop.

In Ireland, they have partnered with Saint Vincent de Paul and local charity shops to help 800 women from the travelling community. The beneficiaries were given vouchers to be redeemed against products for children and family at participating stores.

In Lebanon, AID:Tech partnered with the Irish Red Cross and a local supermarket to help Syrian war refugees living in camps in the city of Tripoli in North Lebanon. $10,000 worth of vouchers were enabled, either via a card distributed by the aid agency staff or via an electronic code sent to their mobile phone. The vouchers were remotely topped-up by the aid agency staff and redeemed at the point of sale via QR code scanning.

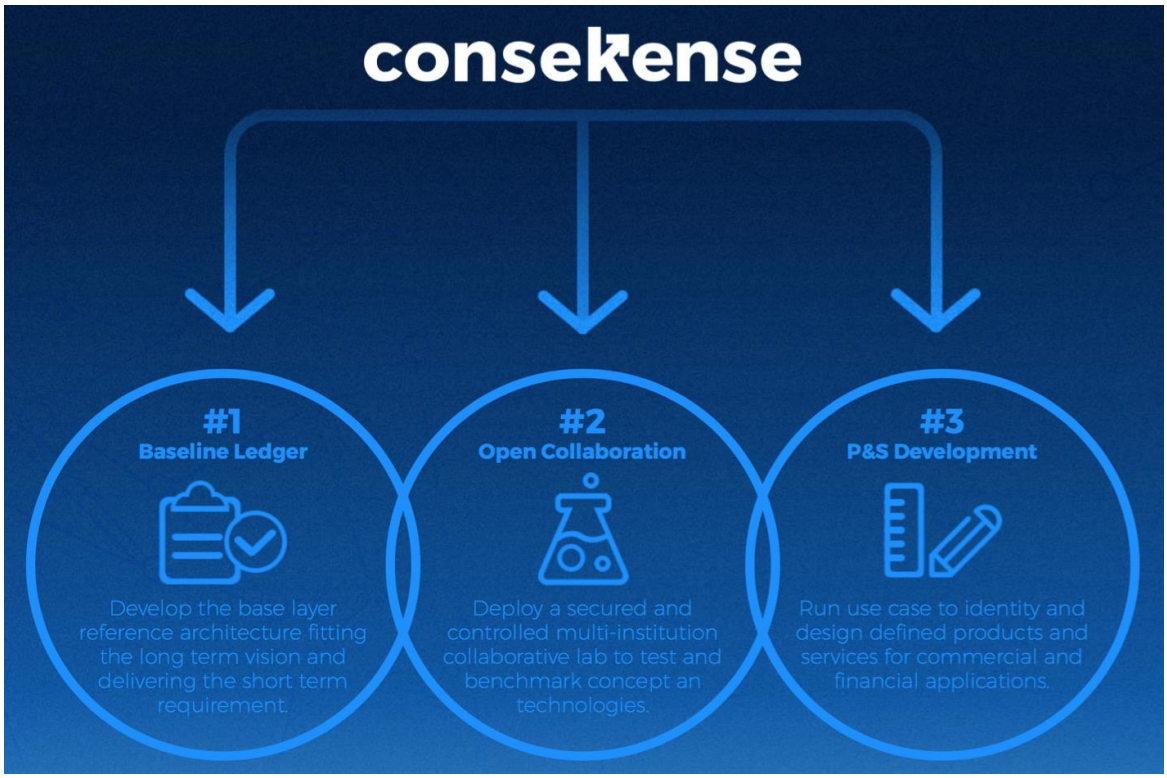
In both cases, and for AID:Tech's future projects, a partnership with mobile operators would be very valuable. The aid or benefits could be directly delivered into users' wallets which would allow the electronic cash distributed to be spent on a much wider variety of services; and the operators distribution network would enable a much wider reach.

Consekense:

Consekense is an open Innovation house running «ConfluenX», an Open API platform allowing worldwide innovators and corporates to connect with Digital Convergence use cases. The Open API platform aggregates new solution stacks to be tested by industry players looking at automate, optimise and transform existing business models with external Innovations.

At the heart, «ConfluenX» is testing value chains relevant to Digital Identity lifecycle, Cyber security and Compliance with products linked to Interoperability, biometrics & strong authentication mechanisms as well as the management of authenticated user data in regard to GDPR regulation and privacy dashboard.

As Consekense is already working with a major mobile operator. GSMA members would benefit to be collaborating with their platform not only as a way to speed the interaction with 3rd parties based in most of the major technology hubs, but as a Sandbox to take advantage of the platform capabilities. For countries where Mobile Connect is live, there would be the additional benefit of new users being identified registering for further services.


consekense
#1
Baseline Ledger
Develop the base layer reference architecture fitting the long term vision and delivering the short term requirement.
#2
Open Collaboration
Deploy a secured and controlled multi-institution collaborative lab to test and benchmark concept an technologies.
#3
P&S Development
Run use case to identity and design defined products and services for commercial and financial applications.

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at www.gsma.com. Follow the GSMA on Twitter: @GSMA.

About Nicolas Steiner, representative of FINTECH Circle:

Nicolas Steiner is a former Telecom executive, investor & serial entrepreneur. Based in London, he represents the Swiss Entrepreneurship Institute and the Silicon Valley based CCICE. He founded TWIXIS Ventures in 2007 and is currently a partner at StartupHome a founding member of Level39 & FINTECH Circle and runs the Digital Ecosystem of the innovation arm of the Group. In these contexts, he has been asked by the GSMA to provide market insights.

For more information, please visit the TWIXIS Ventures website at www.twixis.com. Follow Nicolas Steiner on Twitter: @follow_nicolas

FINTECH Circle is the largest Business Angel Network dedicated to FINTECH in Europe. Its Innovation arm is helping Corporate to connect and engage with the FinTech ecosystem. FINTECH Circle connection with the Cape Innovation and Technology Initiative based in South Africa has been leveraged to ensure scouting relevant Value Chains.

Level39 is Europe's largest technology accelerator for finance, retail, cyber-security and future cities technology companies. Collaborating with Level39, the Entrepreneurship institute managed by the Management School of Fribourg in Switzerland and the Chamber of Commerce International Consortium for entrepreneurs based at the Silicon Valley have been involved in providing insights.

StartupHome operates co-living spaces for startupers, freelancers and entrepreneurs in Europe and USA. These “homes” provides affordable housing for entrepreneurs while facilitating direct link to the Innovation ecosystem. StartupHome provides house for segmented audiences such a house dedicated to Fintech with a Blockchain Lab, others dedicated to FoodTech or for Woman entrepreneur in Technology.