Technology Building Blocks for an Open API Strategy

Lesley-Ann Vaughan, Claudia McKay, and Michel Hanouch

April 2020

CGAP

Introduction

Why open APIs?

Digital financial services (DFS) providers are opening APIs to make it easier for third parties to connect in a seamless, fast, and secure self-service manner. They hope to accelerate growth, increase revenue, and expand the DFS ecosystem.

"Third parties" is the term we use for businesses that integrate with DFS providers' APIs to build applications and products. They can be enterprises, start-ups, developers, nonprofits, or government agencies.

CGAP's vision is that low-income customers will have access to a wider range of relevant and easily usable financial and nonfinancial services, through DFS providers and third parties working collaboratively.

Why review this deck?

A combination of people, processes, and technology change is required to deliver open APIs well.

Too often, business leaders do not engage effectively on key technology considerations, and business strategy is kept separate from technology strategy. Lack of proper integration between business and technology strategy at the design stage can lead to technically unreliable solutions, the need for ongoing intensive technical support to the third parties, and a need to manage financial risk when things go wrong.

This deck aims to bridge the gulf between the business leaders responsible for overall open API strategy and the technology decisions that need to be made. It is part of a collection of practical tools and resources that CGAP is publishing on open APIs.

To see the full collection, visit **the CGAP Open API Collection**.

Who?

This deck focuses on DFS provider business leaders who are responsible for the overall open API strategy within their organizations. It is assumed that the organization already has decided to pursue an open API strategy.

This deck will help business leaders:

- Be clear in what they are expecting of the IT team and why.
- Have confidence they are asking the right questions.
- Guide the open API strategy so that it moves the organization toward digital transformation rather than simply to a digital version of "as is" thinking.

This is introductory material. A variety of excellent resources aimed at a deeper technical level already are available, and some are referenced in the deck.

© CGAP 2019

Structure of the deck

1

Optimizing the third-party journey

Third parties go on a journey from awareness to onboarding to active use of APIs. This section highlights areas DFS providers should prioritize to ensure third parties progress swiftly through each phase.

2

Other technology decisions

The experiences of CGAP's API partners show how DFS providers have answered technology questions that are not third-party and customer facing but have budgetary and security implications.

3

API technology building blocks

This section covers the key components DFS providers need such as the Developer Portal and Sandbox. Start here if you want some terminology explainers.

CGAP

© CGAP 2019

Three design principles to guide DFS provider open API technology decisions

Self-Service Mindset

The cost to acquire and serve third parties should be efficient at scale.

A self-service mindset enables third parties to onboard themselves with as little intervention as possible from your operational and support teams.

Protect Your Reputation

You must protect your reputation with third parties and with end customers.

Well-designed APIs cannot be built on aging infrastructure without harm to the third-party experience—and subsequent impact on provider reputation.

Similarly, the technology team needs to address risks around security and data privacy coming from the legal, compliance, security, and risk teams.

Awesome Third-Party Experience

Good partnerships are built on the understanding that the success of one party contributes to the success of the other.

Success of a third party relies on the right information and support being available when it needs it in its journey.

CGAP

© CGAP 2019

These design principles affect 14 elements of an open API program

Self-Service Mindset

- Good Documentation
- Robust Sandbox
- Easy Onboarding
- Easy Billing/ Settlement
- Proactive Use of Data

Protect Your Reputation

- Appropriate Security
- Consent by Design
- Reliable Core Systems
- Proportionate Risk Management

Awesome Third-Party Experience

- Clear Value Proposition
- Community Engagement
- Well-Designed APIs
- SLAs* on Service Support
- Tools for Innovation and Growth

CGAP

*Service-level agreements

Note: These design principals are explained in more detail throughout the deck and are summarized on Slide 31.

© CGAP 2019

1. Optimizing the third-party journey

Third parties go on a journey from awareness to onboarding to active use of APIs. This section highlights areas DFS providers should prioritize to ensure third parties progress swiftly through each phase.

CGAP

Third-party segments vary in size and maturity

Stand-alone coder

Individuals who code, possibly freelancing from within a hub environment.

May be job hunting rather than building a business.

Looking for the next way to make money from their software skills.

Early-stage innovators

Early-stage start-ups have 1–10 employees and a small customer base. Can be B2B* or B2C.†

Typically pre-revenue. May have won some competitions, prizes, and/or grant funding.

Growth seekers

Businesses that have a customer base and a path to sustainability. May generate revenue and/or be VC funded.

Focused on expanding services to a larger customer base, adjacent services, and more geographies.

Enterprises

Large businesses with thousands of employees, often operating across several countries.

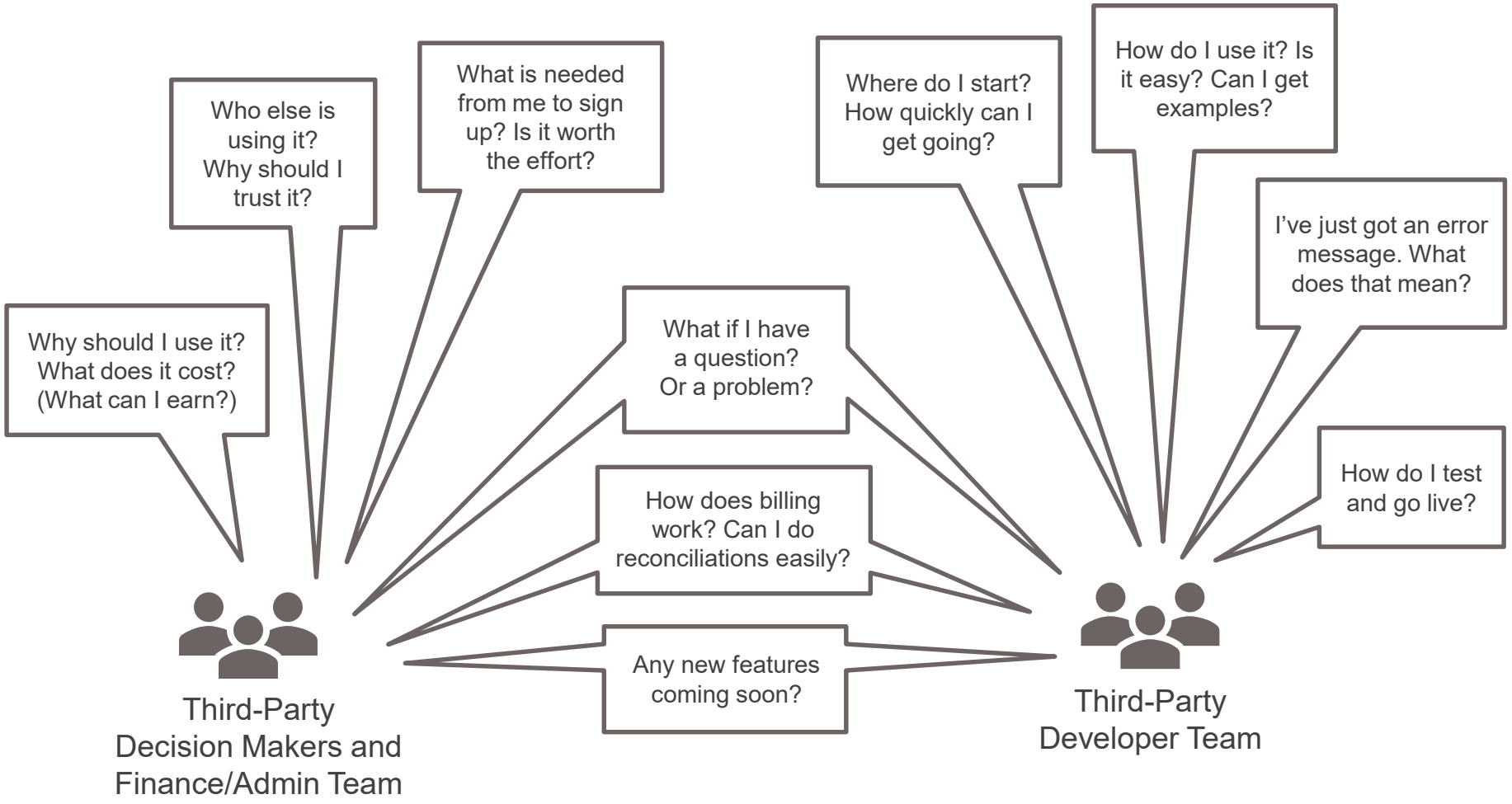
Irrespective of size, third parties want a seamless integration process with online technical tools and support forums that minimize their reliance on the DFS provider's internal teams and processes. They want a safe and secure integration and a way to test before going live. And, when they go live, their needs change.

CGAP

*Business to business; †Business to consumer

© CGAP 2019

Providers need to respond to business and technical questions from third parties

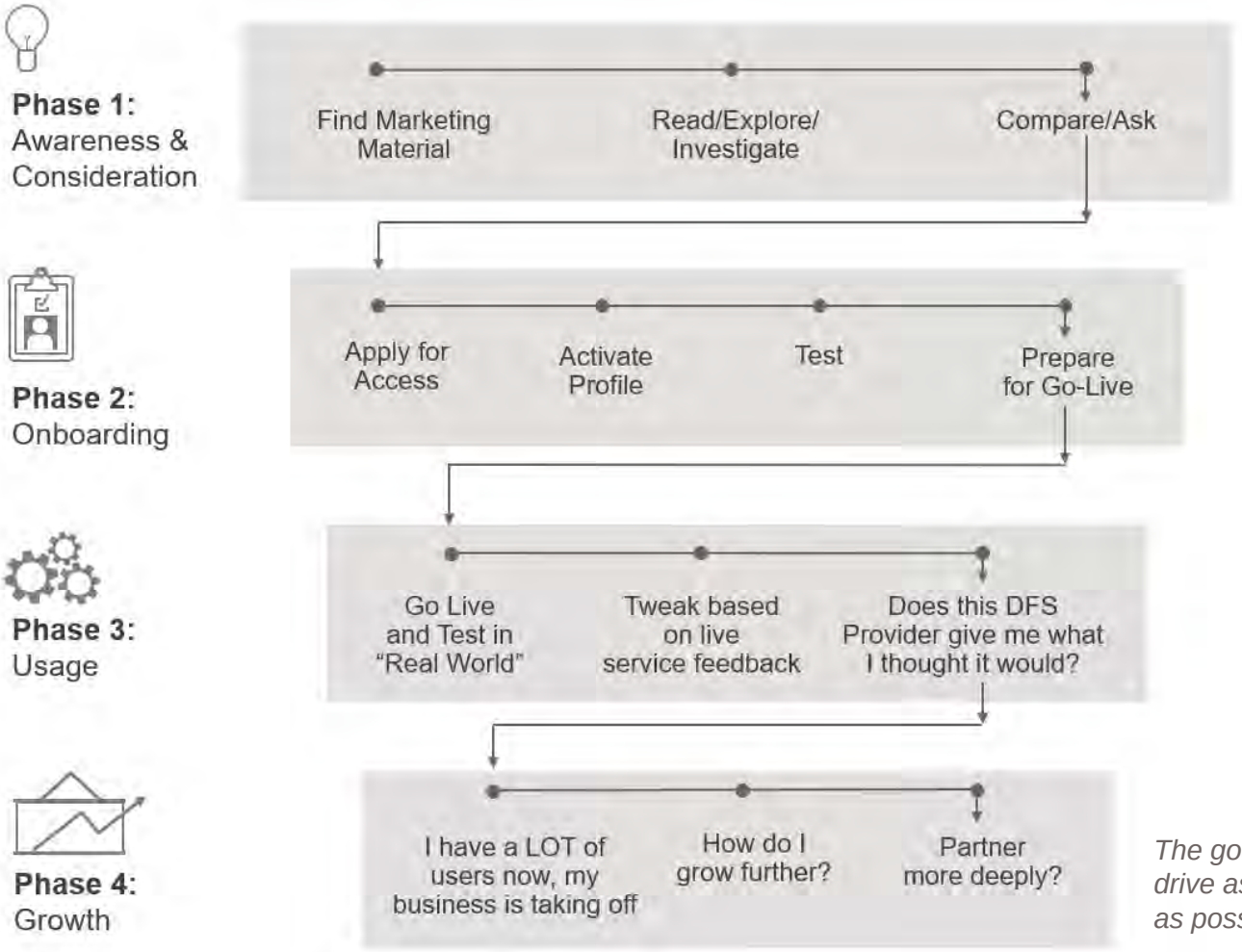


Developers may be employees or contractors of a third-party business. A developer will lead business decisions only sometimes.

© CGAP 2019

The third-party journey

Third parties will go through a process from awareness to active use and growth. Inevitably, there will be some drop-off at each phase.



The goal is to efficiently drive as many third parties as possible toward Phase 4.

© CGAP 2019

Each phase has specific goals for DFS providers

	PHASE FOR THIRD PARTY	GOALS FOR DFS PROVIDER
	**Phase 1:** Awareness and consideration	• Make it easy for third parties to understand what is being offered.
	**Phase 2:** Onboarding	• Make the sign-up process transparent and easy for third parties. • Reduce cost and time of processing applications for DFS providers. • Reduce cost and time for security provisioning for DFS providers and third parties.
	**Phase 3:** Use	• Increase speed to market for a live service for third parties while limiting risk. • Reduce time and cost of billing and settlement.
	**Phase 4:** Growth	• Manage performance at scale. • Support third parties in their growth.

© CGAP 2019

Third-Party Journey

Phase 1: Awareness and Consideration

Find Marketing Material	Read/Explore/ Investigate	Compare/Ask
Why should I use it? What does it cost? Will I make more money?	How do I use it? Can I get examples? What can it really do?	Who else is using it? Why should I trust it?

Goal for DFS providers:

Make it easy for third parties to understand what is being offered.

Technology needs and practical advice

Technology Needs

A developer portal is a website that supports access to APIs. It usually hosts all the information on the APIs and instructions for how to use them and how to access the sandbox.

Ideally, it also will enable users to ask questions and provide clear instructions on how to apply for access.

Practical Advice

Clear Value Proposition

Help decision makers understand the value proposition, the pricing, and terms and conditions. If you are targeting smaller third parties, like standalone coders and early-stage innovators, this is best done via a website.

Community Engagement

A community signals APIs are valuable and encourages community members to help each other and support new members. Slack and WhatsApp/ Telegram groups often work well.

Well-Designed APIs

APIs need to be designed from the perspective of the third party. A developer portal will allow review of code and examples of how to use it that will inspire readers to use them.

Good Documentation

Developers are problem solvers. If the documentation is clear and accurate, and code samples and get-started guides are available, they probably won't ask for much help.

© CGAP 2019

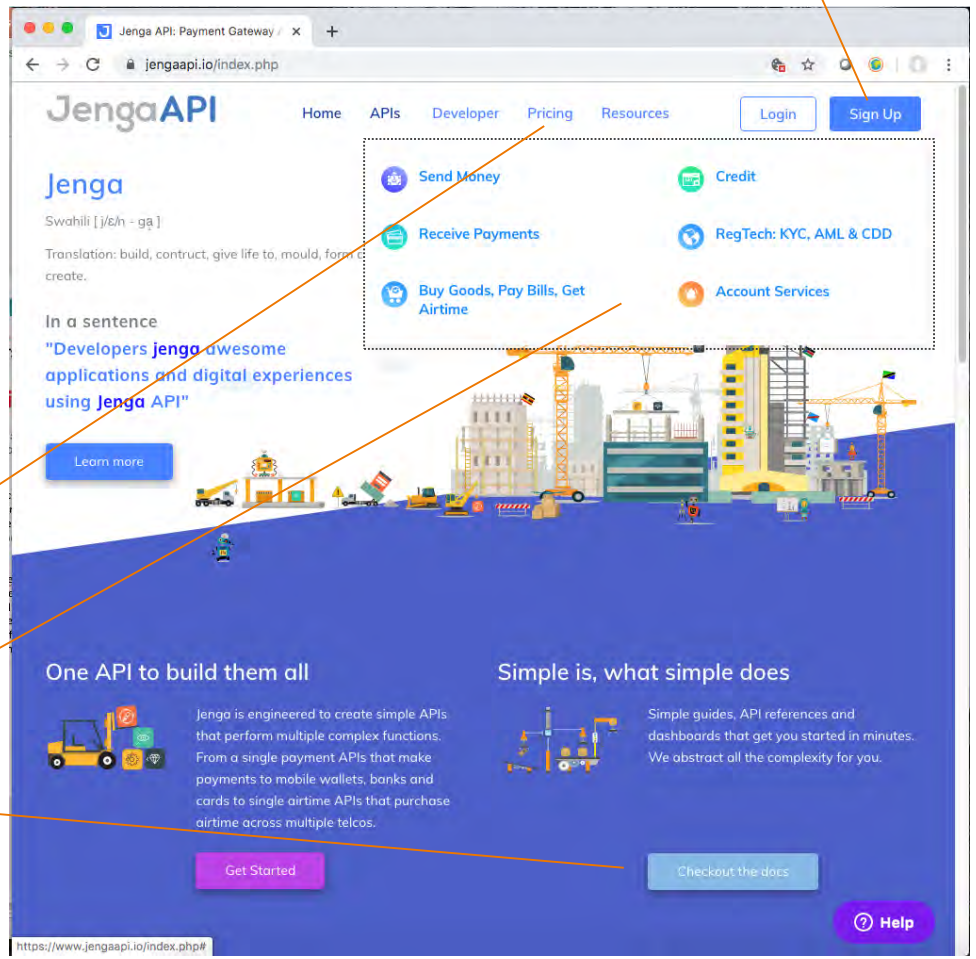
Engage your audience from the outset

Finserve in Africa clearly explains the offer to business and technical team members of third parties on its website.

Finserve
A Fintech subsidiary of Equity Group

Finserve's developer portal (JengaAPI) ensures site visitors understand the offering and how to get started.

Because Finserve offers several value propositions, it has subsites that describe in detail the different services on offer, accessed from the main menu.



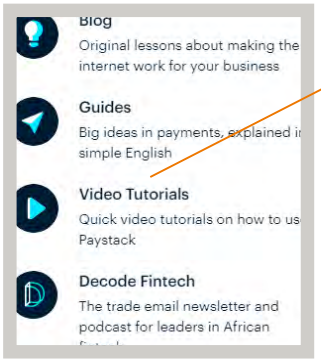
Source: https://www.jengaapi.io/

© CGAP 2019

Use platforms that developers already use to reach the community

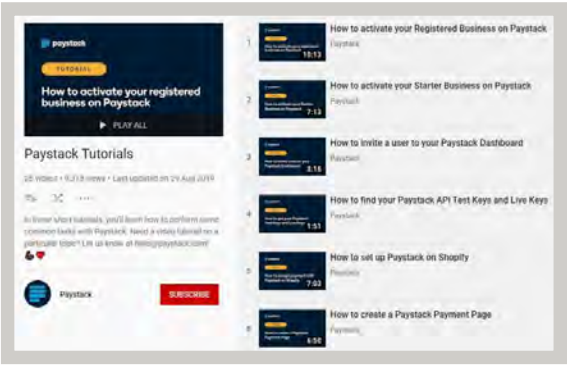
Paystack helps developers through Youtube video tutorials and uses Slack to engage. MTN has created Whatsapp and Skype community support groups. Stripe uses Github.

paystack Paystack is a Nigerian payments provider.

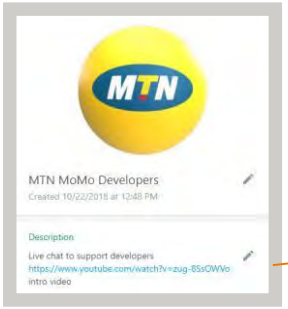


Blogs, tutorials, and guides make the process easier

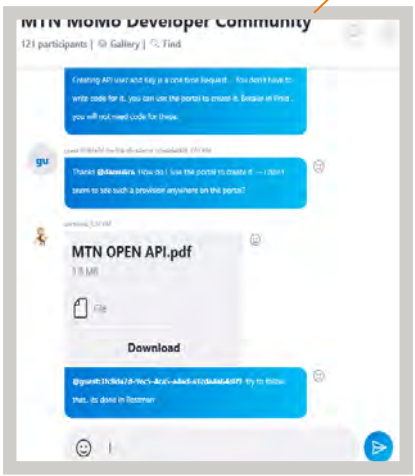
Tutorials hosted on YouTube



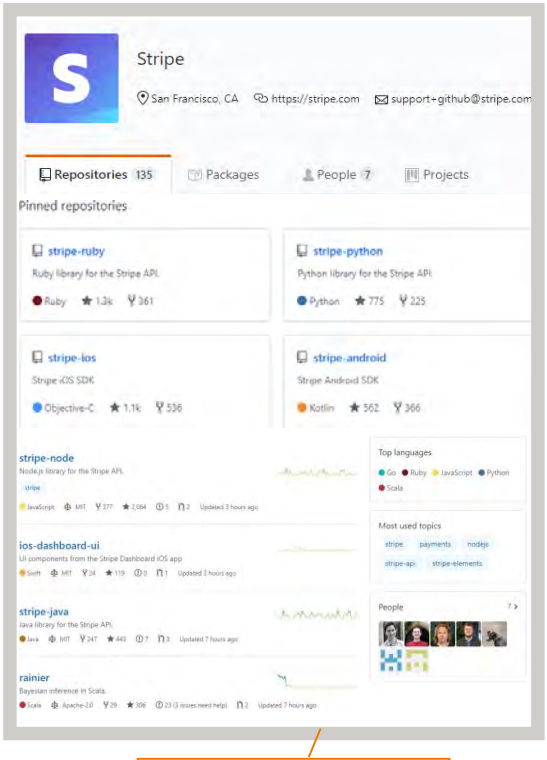
MTN MTN is the largest telecom company in Uganda.



MTN Uganda portal links to WhatsApp and Skype groups, which act as forums for developers



stripe Stripe is a third-party payments processor.



Stripe has moderated forums hosted on GitHub, with multiple contributions across repositories

CGAP

Source: https://bit.ly/36SeY2v, https://momodeveloper.mtn.com/contact-support, https://github.com/stripe

© CGAP 2019

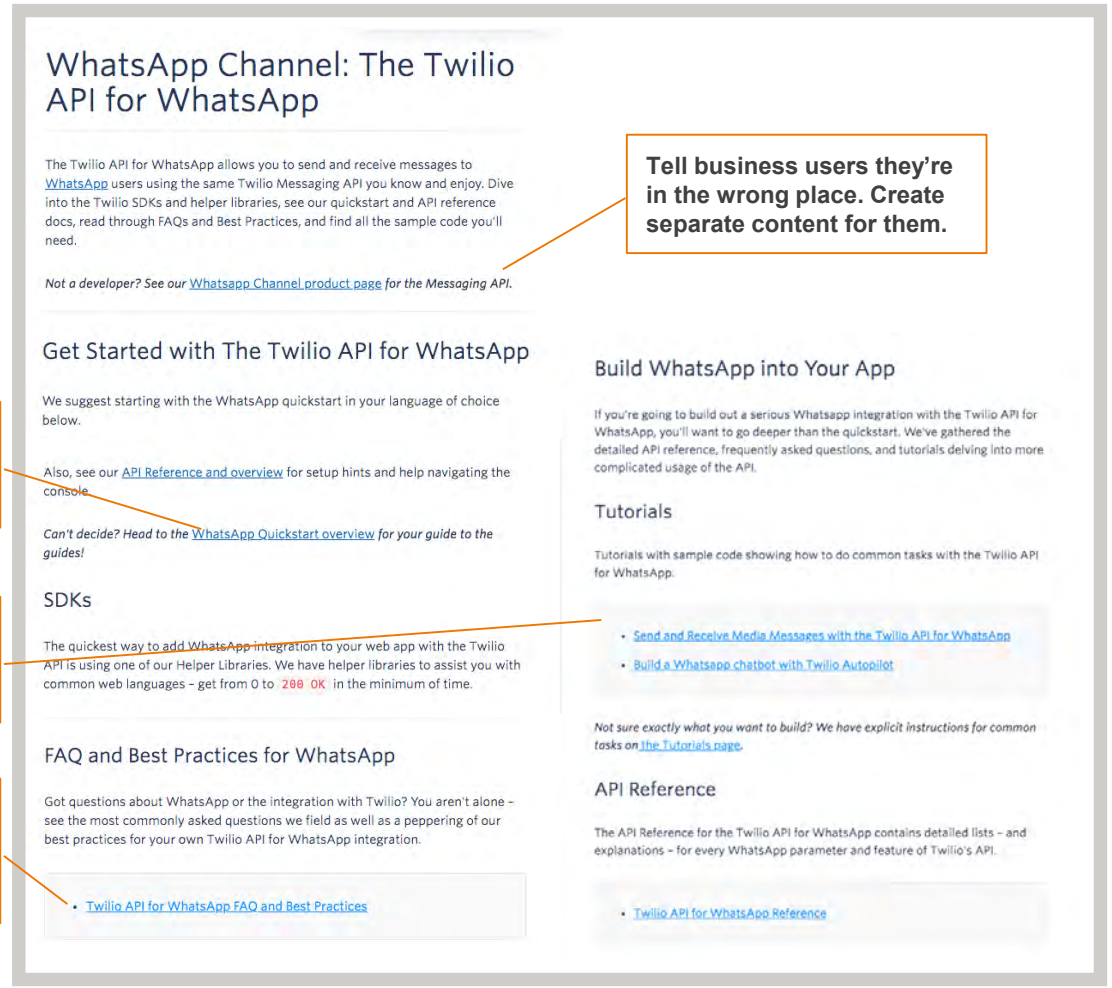
Generate business through good documentation

Twilio's developer documentation drives third-party engagement.

Cloud communications platform as a service company

Twilio sees developer documentation as a product to drive third-party engagement, not as a peripheral background activity.

A tip from Twilio: "If the documents say too much, [developers] assume they have a lot to do."



Source: https://www.twilio.com/docs/sms/whatsapp/; https://eventil.com/talks/PPSznP-jarod-reyes-how-twilio-writes-documentation

© CGAP 2019

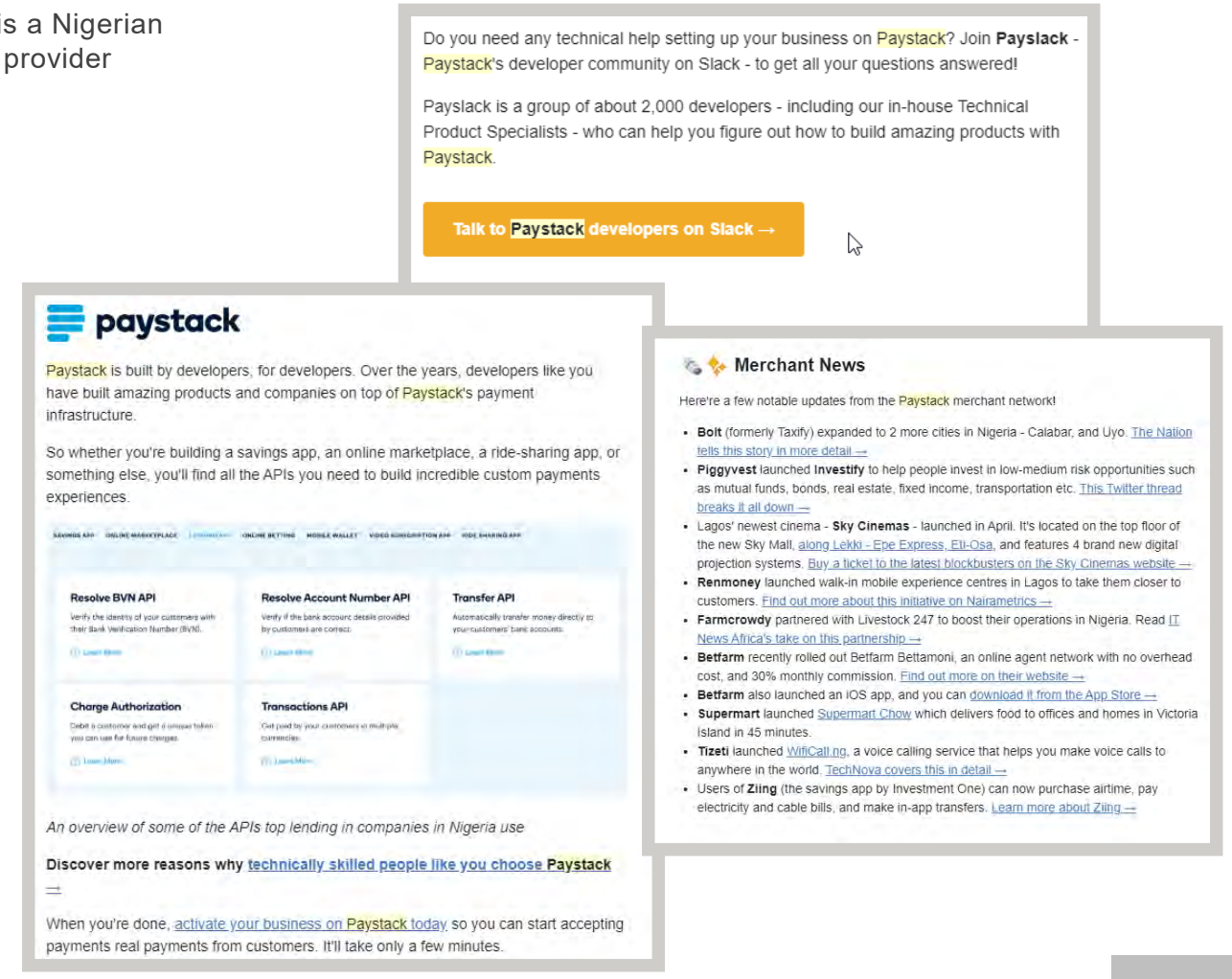
Reduce third-party dropout

Paystack's email marketing campaign encourages parties to continue the onboarding process.

Paystack is a Nigerian payments provider

Paystack has created an effective automated email campaign that developers can use in the first four weeks after registration. This helps developers learn about Paystack and be inspired by stories from Paystack merchants.

This is an example of using marketing technology and lead generation management to encourage businesses to keep trying and to get help if they need it.



Do you need any technical help setting up your business on Paystack? Join **Payslack** - Paystack's developer community on Slack - to get all your questions answered!

Payslack is a group of about 2,000 developers - including our in-house Technical Product Specialists - who can help you figure out how to build amazing products with Paystack.

Talk to Paystack developers on Slack →

paystack

Paystack is built by developers, for developers. Over the years, developers like you have built amazing products and companies on top of Paystack's payment infrastructure.

So whether you're building a savings app, an online marketplace, a ride-sharing app, or something else, you'll find all the APIs you need to build incredible custom payments experiences.

Resolve BVN API

Verify the identity of your customers with their Bank Verification Number (BVN).

Resolve Account Number API

Verify if the bank account details provided by customers are correct.

Transfer API

Automatically transfer money directly to your customers' bank accounts.

Charge Authorization

Debit a customer and get a unique token you can use for future charges.

Transactions API

Get paid by your customers in multiple currencies.

An overview of some of the APIs top lending in companies in Nigeria use

Discover more reasons why technically skilled people like you choose Paystack →

When you're done, activate your business on Paystack today so you can start accepting payments real payments from customers. It'll take only a few minutes.

Merchant News

Here're a few notable updates from the Paystack merchant network!

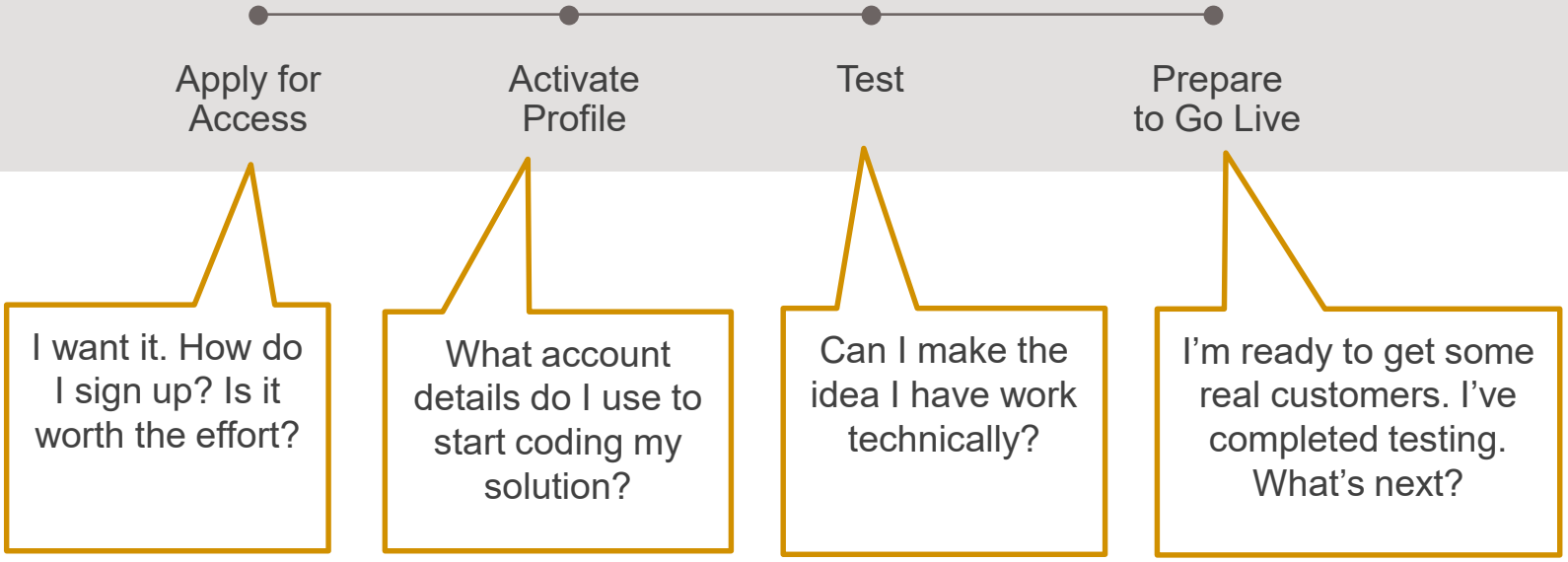
- **Bolt** (formerly Taxify) expanded to 2 more cities in Nigeria - Calabar, and Uyo. The Nation tells this story in more detail →
- **Piggyvest** launched **Investify** to help people invest in low-medium risk opportunities such as mutual funds, bonds, real estate, fixed income, transportation etc. This Twitter thread breaks it all down →
- Lagos' newest cinema - **Sky Cinemas** - launched in April. It's located on the top floor of the new Sky Mall, along Lekki - Epe Express, Eti-Osa, and features 4 brand new digital projection systems. Buy a ticket to the latest blockbusters on the Sky Cinemas website →
- **Renmoney** launched walk-in mobile experience centres in Lagos to take them closer to customers. Find out more about this initiative on Nairametrics →
- **Farmcrowdy** partnered with Livestock 247 to boost their operations in Nigeria. Read IT News Africa's take on this partnership →
- **Betfarm** recently rolled out Betfarm Bettamoni, an online agent network with no overhead cost, and 30% monthly commission. Find out more on their website →
- **Betfarm** also launched an iOS app, and you can download it from the App Store →
- **Supermart** launched Supermart Chow which delivers food to offices and homes in Victoria Island in 45 minutes.
- **Tizeti** launched WifiCall.ng, a voice calling service that helps you make voice calls to anywhere in the world. TechNova covers this in detail →
- Users of **Ziing** (the savings app by Investment One) can now purchase airtime, pay electricity and cable bills, and make in-app transfers. Learn more about Ziing →

Source: Paystack email marketing

© CGAP 2019

Third-Party Journey

Phase 2: Onboarding



Goals for DFS providers:

- Make the sign-up process transparent and easy for third parties.
- Reduce cost and time of processing applications for DFS provider.
- Reduce cost and time for security provisioning for providers and third parties.

Technology needs and practical advice

Technology Needs

- A sandbox that allows users to fully test their own system before they go live.
- A way to manage the process of applying for access (including any queries that arise) via a support system.
- An API management platform to deliver security features that allow risk and compliance teams to authorize equally secure yet faster and cheaper onboarding practices.

Practical Advice

SLAs on Service Support

Most platforms use a standard ticketing service to allow visitors to ask questions. Many platforms use something like Zendesk or Intercom.

Easy Onboarding

The biggest barriers to entry for external innovators are opaque processes that can feel deliberately difficult. Ensure the process is easy for third parties to understand and that SLAs are in place and work to improve this process over time with legal, risk, and compliance teams involved.

Appropriate Security

The security architecture should remove overly burdensome and costly requirements to establish a secure connection. Today's method (typically a secure direct connection) is outdated. Use guidance from experts for an up-to-date security architecture.

Robust Sandbox

The sandbox allows developers to experience the behavior of the core system in a test environment. It should simulate live system behavior and let third parties test what works and simulate errors to design software when it doesn't.

© CGAP 2019

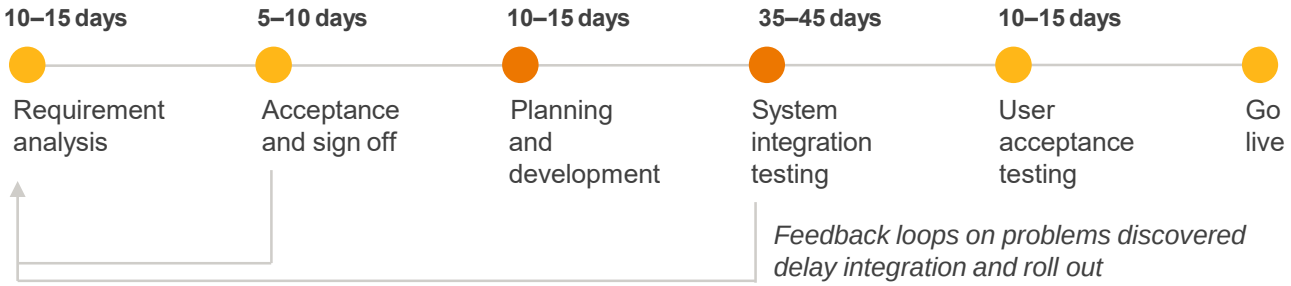
Reduce cost and time of processing applications

MTN Uganda streamlined the process of onboarding third parties. It launched its developer portal in October 2018. Self-service access and changes to the approvals process helped it to reduce time to market. This took 32 days at launch, and the team hopes to reduce this further to about 5 days. It can now tell third parties the targeted number of days per step on its portal to help them understand what to expect.

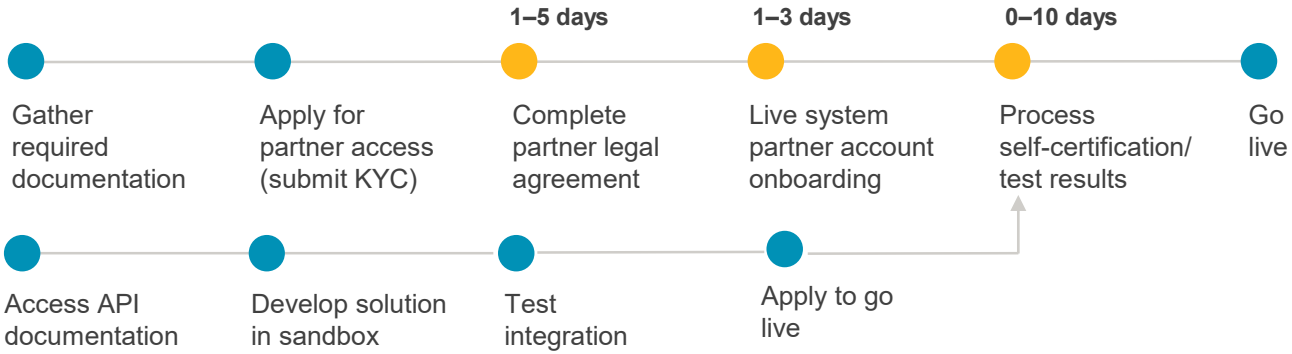
ILLUSTRATIVE EXAMPLE

Controlled and led by DFS provider | Tech integration collaboration | Controlled and led by third party

Process without self-service, minimum 90 days



Process with self-service, average 2–20 days



The technical team works in parallel to the business legal requirements processing, which allows things to move swiftly.

Source: CGAP analysis from work with partner DFS providers

© CGAP 2019

Facilitate self-service developer verification

Safaricom's developer portal allows third-party business owners to verify developers during onboarding in a self-service way, with no involvement from Safaricom staff.

Third-party business owners use the self-service feature to verify the identity of developers before giving them access to live system developer keys.

This allows the process of onboarding the business to be decoupled from the process of onboarding a developer and removes the expectation that a nontechnical resource at a business will deliver developer keys securely.

The onboarding process digitally connects the two parties via a one-time PIN (OTP) verification process before access to the live system is granted.

Safaricom's M-PESA is based in Kenya and is one of the largest and most successful mobile money services in the world.

Developer completes a form with the full details of the registered business owner.

↓

Business owner is notified of the request and an OTP is sent to his/her registered number.

↓

Developer retrieves OTP sent to the business owner and enters it in the developer portal to verify the relationship.

↓

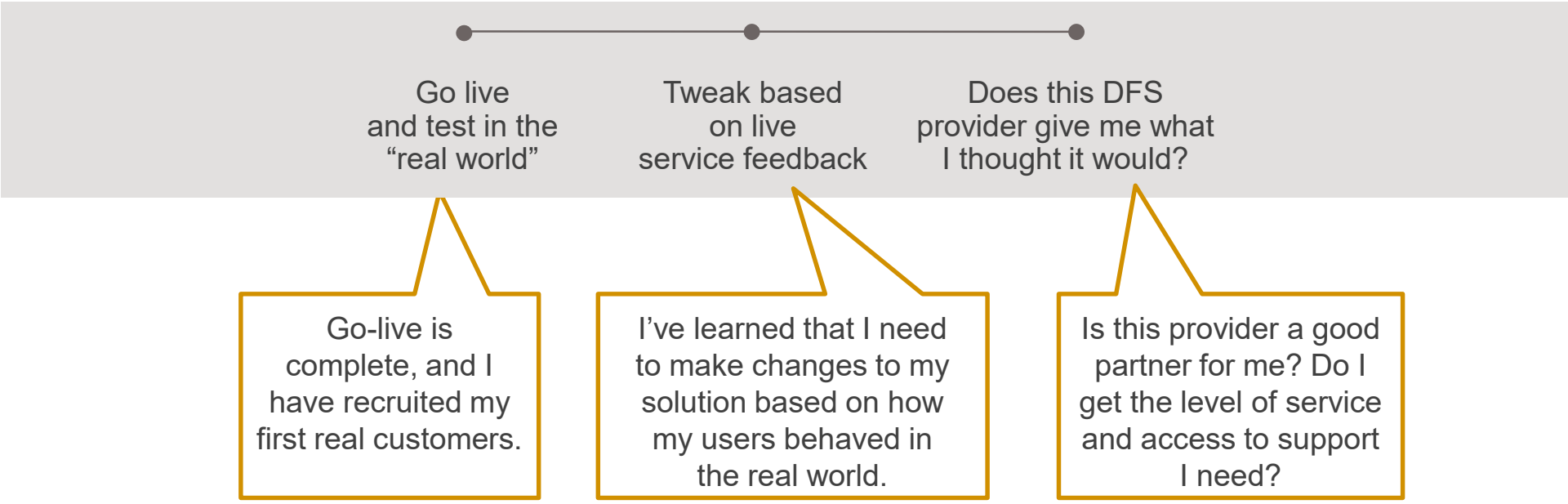
Developer moves to the next step of the onboarding process and consent granted is stored digitally.

Source: CGAP analysis of Safaricom developer onboarding experience; https://developer.safaricom.co.ke/.

© CGAP 2019

Third-Party Journey

Phase 3: Use



Goals for DFS providers:

- Increase speed to market for third parties while limiting risk.
- Reduce time and cost of billing and settlement.

Technology needs and practical advice

Technology Needs

- Process automation technology for developer verification.
- Technology configured so that it complies with API management policies. (e.g., to manage risk through throttled access).
- Good use of data for process automation for settlement and compliance management.

Practical Advice

Consent by Design

Technology is needed to manage the process of getting and revoking consent from customers. It needs to ensure customers can stay in control and that there is a "single source of truth."

Proportionate Risk Management

A risk-based, controlled approach to scale requires new rules: e.g., solutions with lower KYC requirements should be capacity limited and the DFS provider should be able to deny access swiftly to one solution independent of others.

Easy Billing/ Settlement

To reach scale, data analytics on any risk controls related to settlement should be automated. They should not rely on manual checks ahead of payouts.

This process is not burdensome if scale is planned for digitally, including clarity for financial liability when things go wrong.

© CGAP 2019

Manage customer consent

Starling Bank is a digital, mobile-only challenger bank in the United Kingdom.

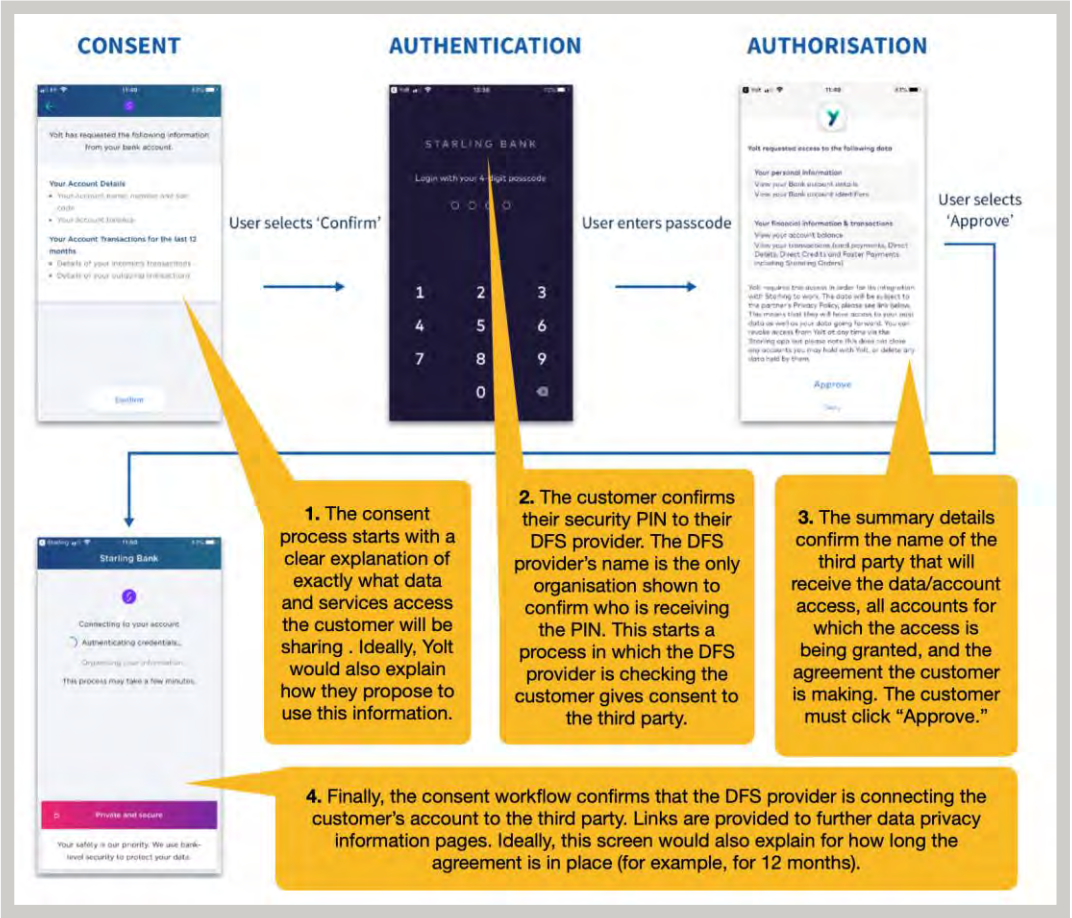
Yolt is an app that allows users to manage money and budgets better.

Starling Bank's open APIs enable third parties to connect to customers' bank accounts.

When a Starling Bank customer seeks to link their bank account to Yolt via the company's app, the app redirects them to the Starling Bank consent workflow.

At this stage, Starling Bank clearly explains to the customer what data and level of account access they will be sharing with Yolt, and the customer must authorize an agreement.

Customers can revoke access at any time through the Starling Bank app.



Source: "The UX of Consent Models in Open Banking," Courtney Yule, https://blog.scottlogic.com/2018/08/24/the-ux-of-consent-models-in-open-banking.html

© CGAP 2019

Create a risk-based approach to onboarding third parties

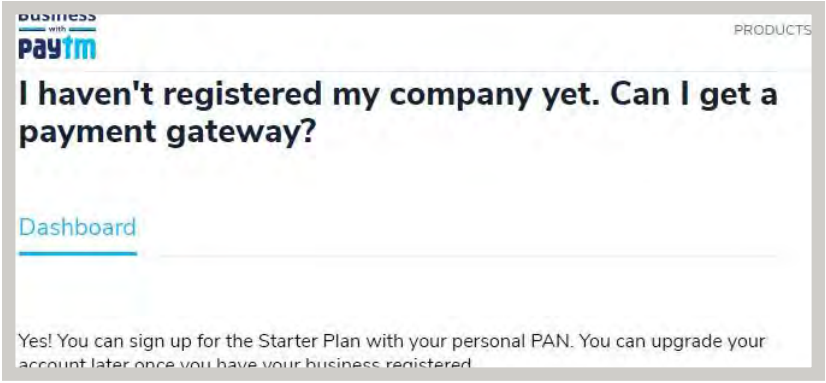
Paytm is one of India's largest ecommerce payments systems and digital wallet companies.

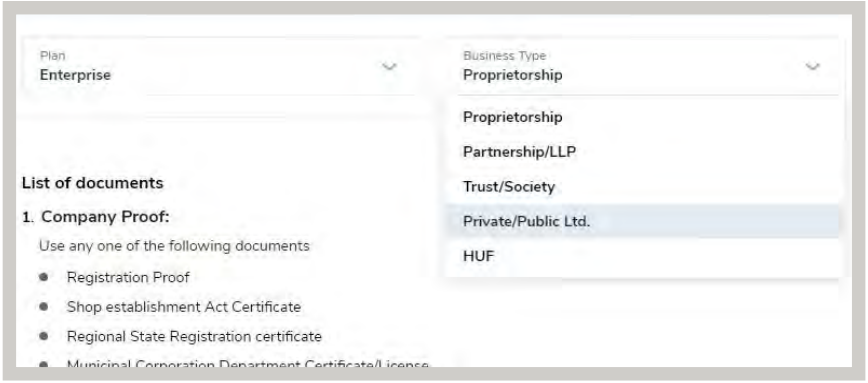
Paytm allows instant activation when individuals/small businesses complete a simple online form and submit a national ID.

This plug-and-play product limits functionality. Use cases are restricted to customer-to-bank payments, and total monthly transactions are limited to less than INR 20,000 (~US$280, the regulatory limit beyond which KYC is needed). This limits Paytm's regulatory, security, and reputational risk.

For other third parties, onboarding/KYC requirements depend on the type of business and their total monthly transaction amount.

For all other cases, Paytm reviews the product integration before going live to mitigate security and reputational risk. It requires KYC depending on the total monthly payment accepted and the type of business registration to mitigate regulatory risk/requirement.





Source: https://paytm.com/.

© CGAP 2019

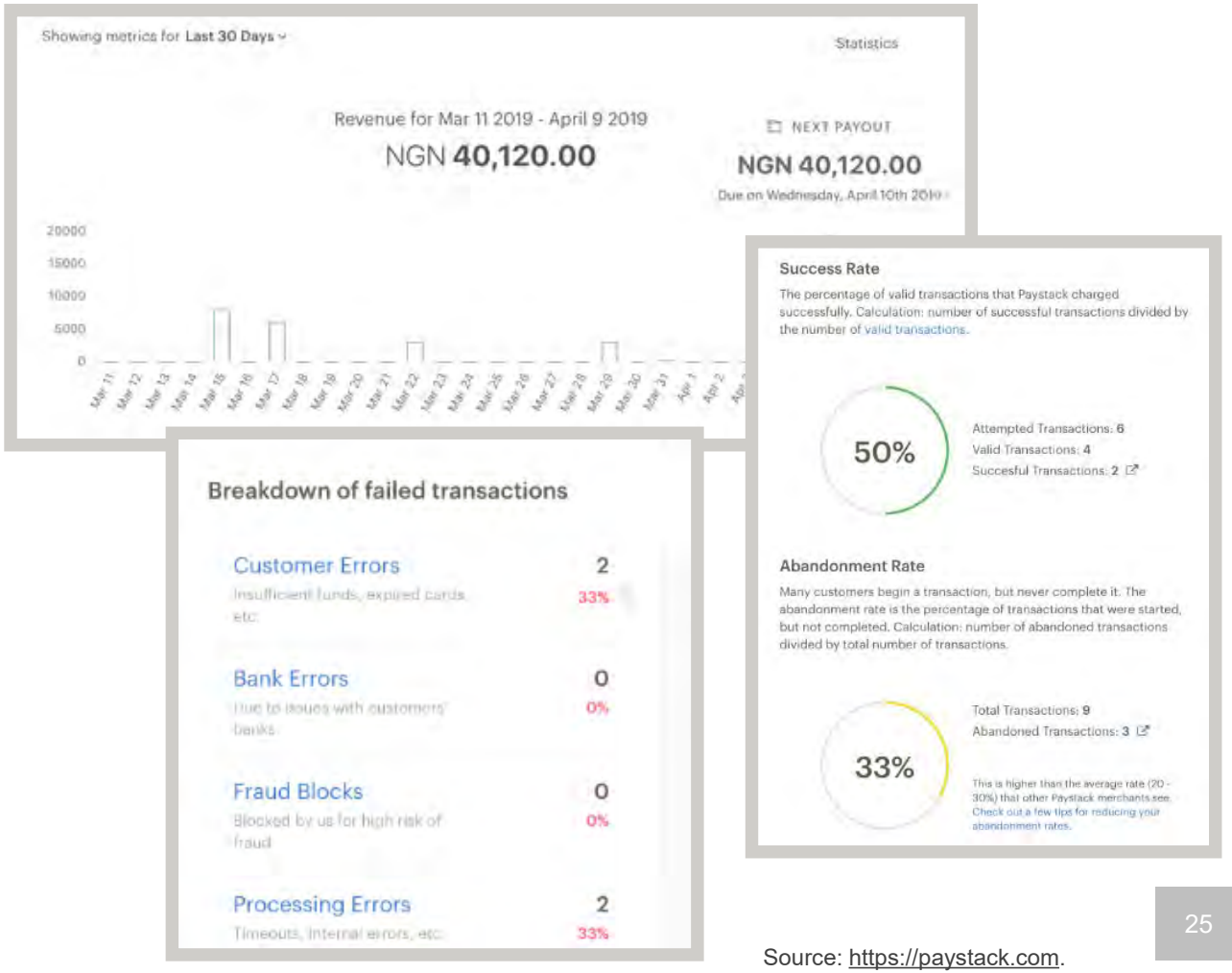
Provide access to user-friendly billing and settlement information

Paystack provides dashboards with important information for third parties.

Paystack gives its third parties information on demand on revenue, settlement, failures, and reasons for failure.

This allows Paystack to automate much of the reconciliation and settlement process and handle dispute management in a data-centered way.

It also helps the third party understand its use of the service.



Source: https://paystack.com.

© CGAP 2019

Third-Party Journey

Phase 4: Growth

I have A LOT of users now. My business is taking off.

How do I grow my business further?

Is it possible to partner more deeply?

This service is important to my business.

How do I ask for improvements? How do I get feedback on my suggested improvements? How long will it take?

Can we talk about partnering more deeply? I'd like to discuss potential opportunities.

Goals for DFS providers:

- Manage performance at scale.
- Support third parties in their growth.

Technology needs and practical advice

Technology Needs

- Responsive performing underlying systems.
- Access to API use self-service data to support business decisions.

Practical Advice

Reliable Core Systems

If the core system does not deliver the performance needed, it puts all the dependent third-party businesses at risk.

Investment in real-time technical monitoring is essential to understand “normal” behavior and find anomalies early, allowing quick reactions to technology failures, breaches, and suspicious activity.

Tools for Innovation and Growth

There are several ways to support third parties to achieve success. One option is to help customers discover third-party services through digital marketplaces. Another option is to co-create a roadmap of additional offerings or business models with the third-party community based on learning how they use the service.

Use of Data

Third parties should be able to access data on their own so they can review how they are using the service, perform reconciliations, and use it for business decisions.

Active use of self-service data can help DFS providers manage risk in business-as-usual activities. In addition, they can get use pattern insights, explore new pricing options, determine follow-on use cases, or make investment decisions.

© CGAP 2019

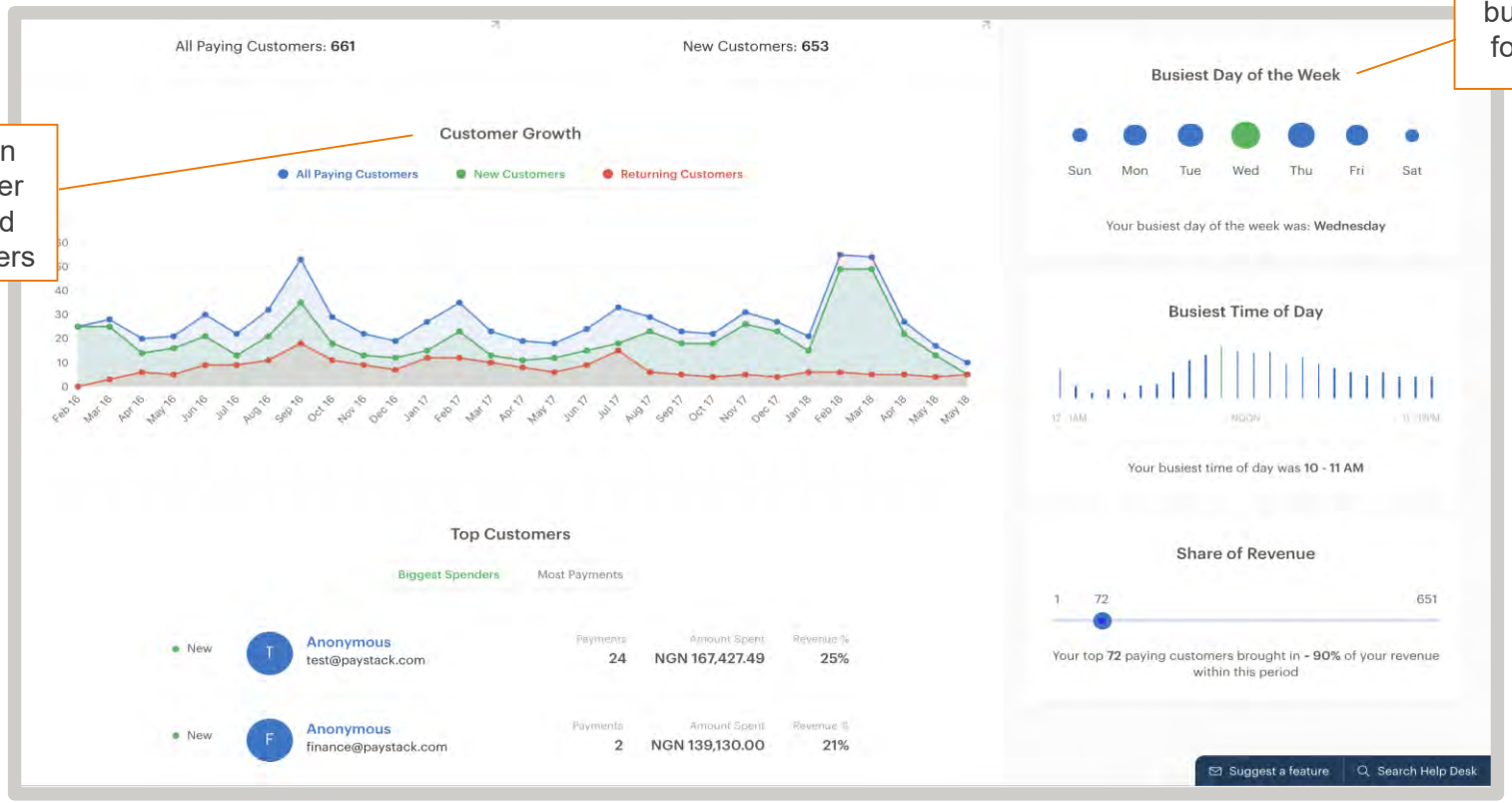
Show third parties information on their API activity

Paystack provides deeper analytics to help third parties understand API use patterns.

paystack Paystack is a Nigerian payments provider.

Information on customer growth and top customers

Data on busiest times for business



Source: "New: Customer Insights and Revamped Customer Directory on the Paystack Dashboard," Paystack, https://paystack.com/blog/product/customer-insights-and-customer-directory.

© CGAP 2019

When APIs fail to deliver

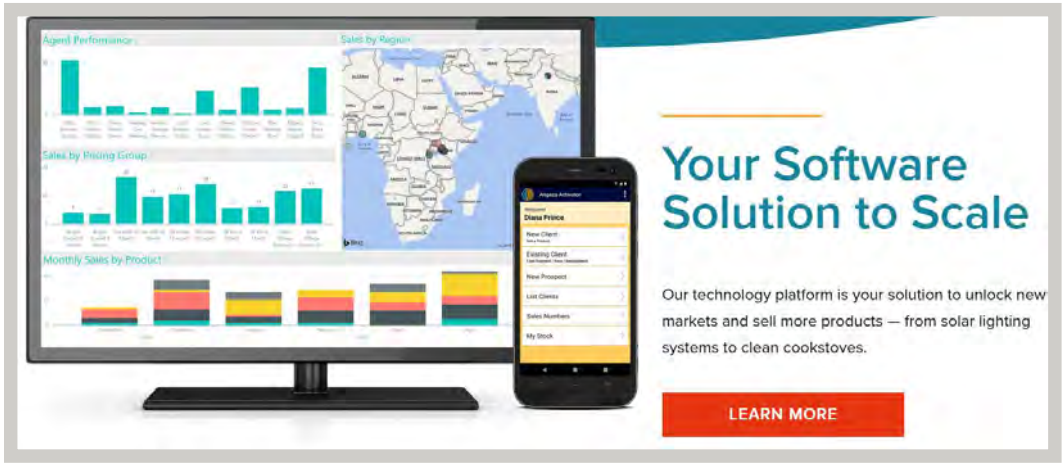
DFS providers must be aware of the impact outages and maintenance windows have on their third-party customer base and the end customers they serve.

Solar PAYGo companies update their customer systems instantly over the air when payments are received.

The business depends on the reliability of the digital money rails and the API that notifies them that payment has been received.

Problems arise if the API is not available due to a maintenance window or an outage or the API says payment was made, but the money doesn't land in the account.

angaza



Angaza provides software solutions, including mobile money payment acceptance, for PAYGo solar distributors.

It estimates that its biggest customer could lose more than $12k per hour if there's a mobile money outage during peak hours. Some will be recovered when the outage is resolved, but the customer's reputation will have been damaged.

Source: Angaza COO, https://www.angaza.com/.

CGAP

© CGAP 2019

Help third parties be digitally discovered

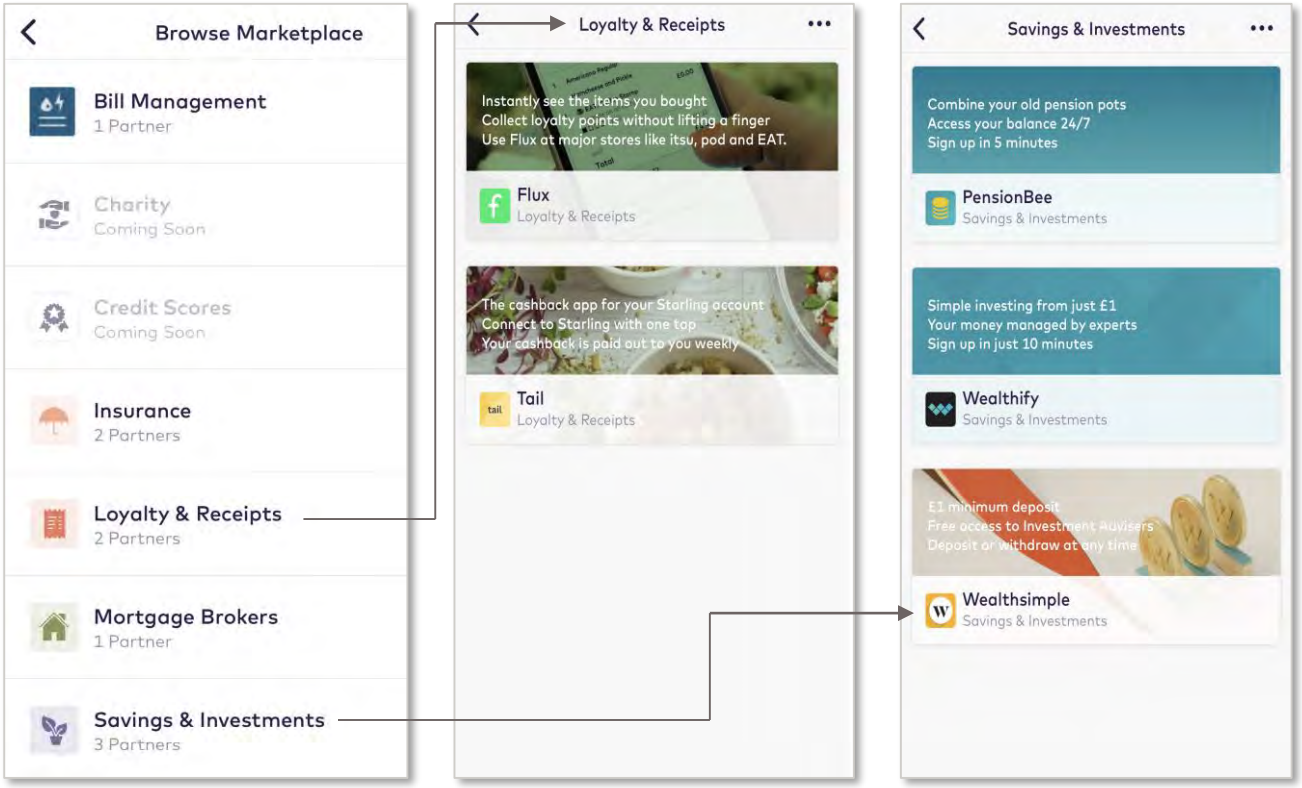
Starling Bank allows customers to find new third parties easily.

STARLING BANK

Starling Bank is a digital, mobile-only challenger bank in the United Kingdom.

It designed its customer app so that it easily can add new third parties and put itself at the center of facilitating third-party connections to its customers.

BTPN Bank in Indonesia similarly is designing changes to its agent app to digitally connect small shopkeepers working as agents to FMCG partners.*



*Fast-moving consumer goods. Source: Starling Bank App.

© CGAP 2019

Design principles for an open API program

DESIGN PRINCIPLE	KEY ELEMENT	DESCRIPTION
Self-Service Mindset 	**Good Documentation**	Developers are problem solvers. They won't ask for much help if the documentation is clear and there are accurate code samples.
	Robust Sandbox	Developers need to test their solution and simulate live system behavior as part of good coding practices.
	Easy Onboarding	An opaque onboarding process is the biggest barrier to entry for third parties.
	Easy Billing/Settlement	The cashflow of businesses depends on swift access to money. If providers are collecting money on behalf of third parties, they need a quick and easy settlement process.
	Proactive Use of Data	Enabling the right employees to gain access to data on their own will allow quick reactions to breaches and suspicious activity. Access to self-service data also will allow teams at the DFS provider and at the third party to uncover new business opportunities.
Protect Your Reputation 	**Appropriate Security**	Security and consumer protection mechanisms need to be standardized to open API best practices in the industry.
	Consent by Design	By ensuring strongly managed consent mechanisms from the outset, it is possible to have a conversation with information security, cybersecurity, and data protection officers on open API innovation while ensuring consumer protection is top of mind.
	Reliable Core Systems	Reliable core systems are necessary for consumer protection, cybersecurity, disaster recovery, fraud management, and much more.
	Proportionate Risk Management	A risk-based, controlled approach to scale requires new rules, and open API platform engineering can support this: e.g., capacity limiting to throttle liability and the ability to swiftly remove access from single connections when required.
Awesome Third-Party Experience 	**Clear Value Proposition**	Third parties need to understand how they can benefit from open APIs.
	Community Engagement	To bring excitement and awareness to the program, the third-party community needs to be made aware of what others are doing and incentivized to innovate.
	Well-Designed APIs	APIs need to be built on modern standards and reliably work to agreed definitions.
	SLAs on Service Support	Third-party support should be done in a similar manner to customer support by using tickets and measuring SLAs to maintain standards as volumes grow.
	Tools for Innovation and Growth	There are several ways to help third parties be successful, from helping end customers to discover services through a marketplace, to co-creating new business models and service offerings.

CGAP

© CGAP 2019

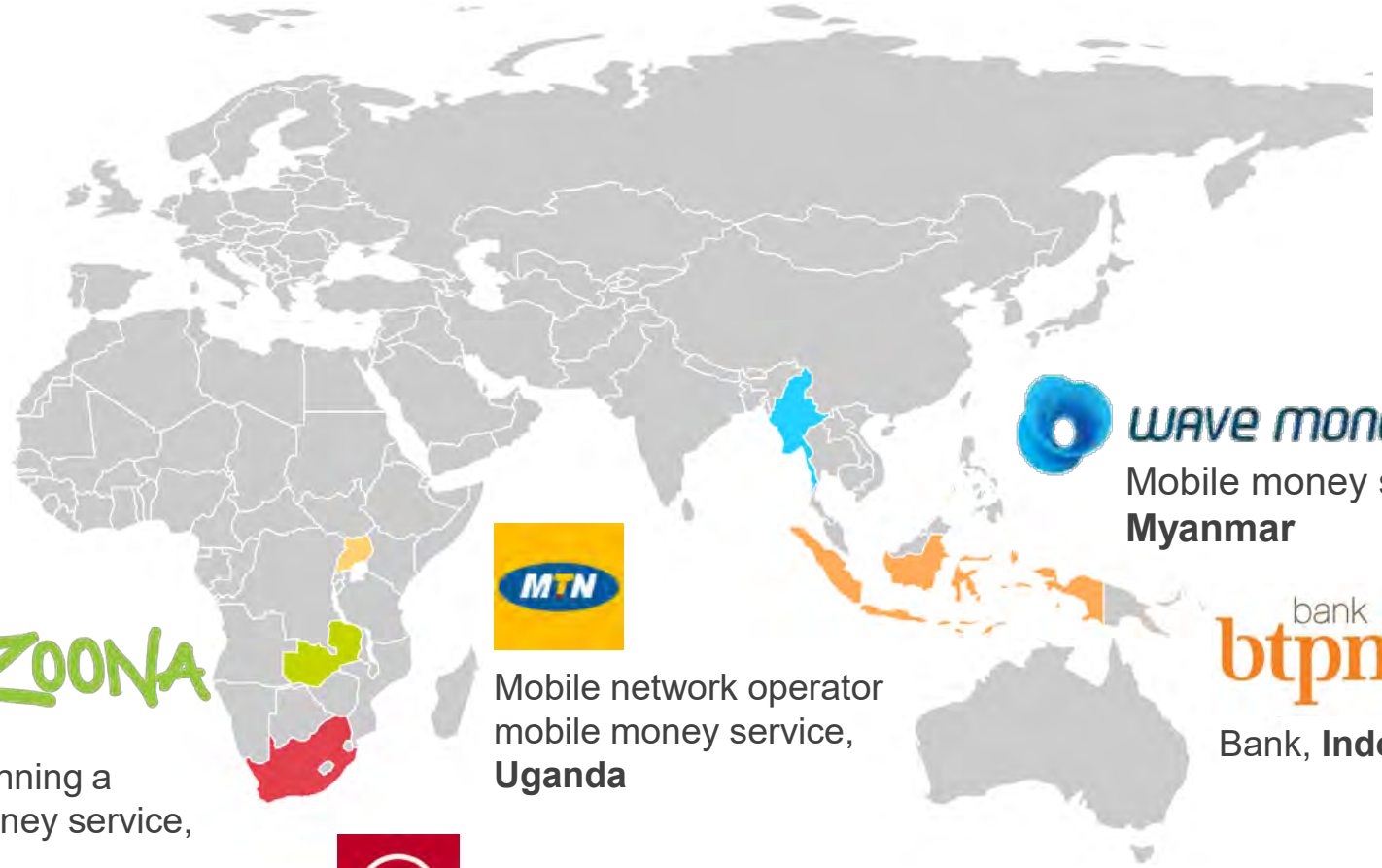
2. Other technology decisions

The experiences of CGAP's API partners show how DFS providers have answered technology questions that are not third-party and customer facing, but have budgetary and security implications.

CGAP

CGAP's open API partners

CGAP worked with 5 DFS providers to support their open API strategies.



Mobile money service, **Myanmar**

Mobile network operator mobile money service, **Uganda**

Bank, **Indonesia**

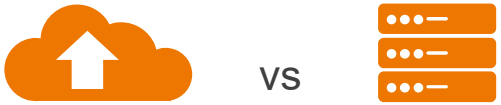
Fintech running a mobile money service, **Zambia**

Bank, **South Africa**

© CGAP 2019

To cloud or not to cloud?

Each CGAP partner had to decide whether to use cloud or locally hosted infrastructure, taking into account regulatory restrictions, company policies, and other factors. Here's what they decided and why.



	ZOONA, ZAMBIA	MTN, UGANDA	BTPN, INDONESIA
Constraint	No business or regulatory constraint	Centralized technology strategy and group-appointed technology vendor	Strict regulatory constraints
API platform chosen	Industry-recognized API management solution Google Apigee, hosted in the Amazon Web Services (AWS), connected with core systems also in AWS	Microsoft Azure, an industry-recognized cloud-hosted platform, connected to the core systems also in Azure	Industry-recognized API management solution (Axway), hosted locally
Reason	Keep initial costs minimal	Led by technology partner preferences	Regulatory constraints prohibited cloud-hosted infrastructure
Implications	A low monthly cost to get going meant an easy decision to invest and try	The same portal is launched in 5 countries within 12 months of original launch	Larger expense and timelines because of need to install locally

Using a cloud-based API management solution: Hosting in the cloud offers benefits of economies of scale, speed to market, and agility. That is why fintechs, neobanks, and start-ups often are designed assuming cloud services will be used natively for the full technology suite.

However, some country regulations and company policies mean cloud can't be used.

CGAP

© CGAP 2019

Build, buy, or partner?

Whatever the choice, some degree of external support likely will be required.

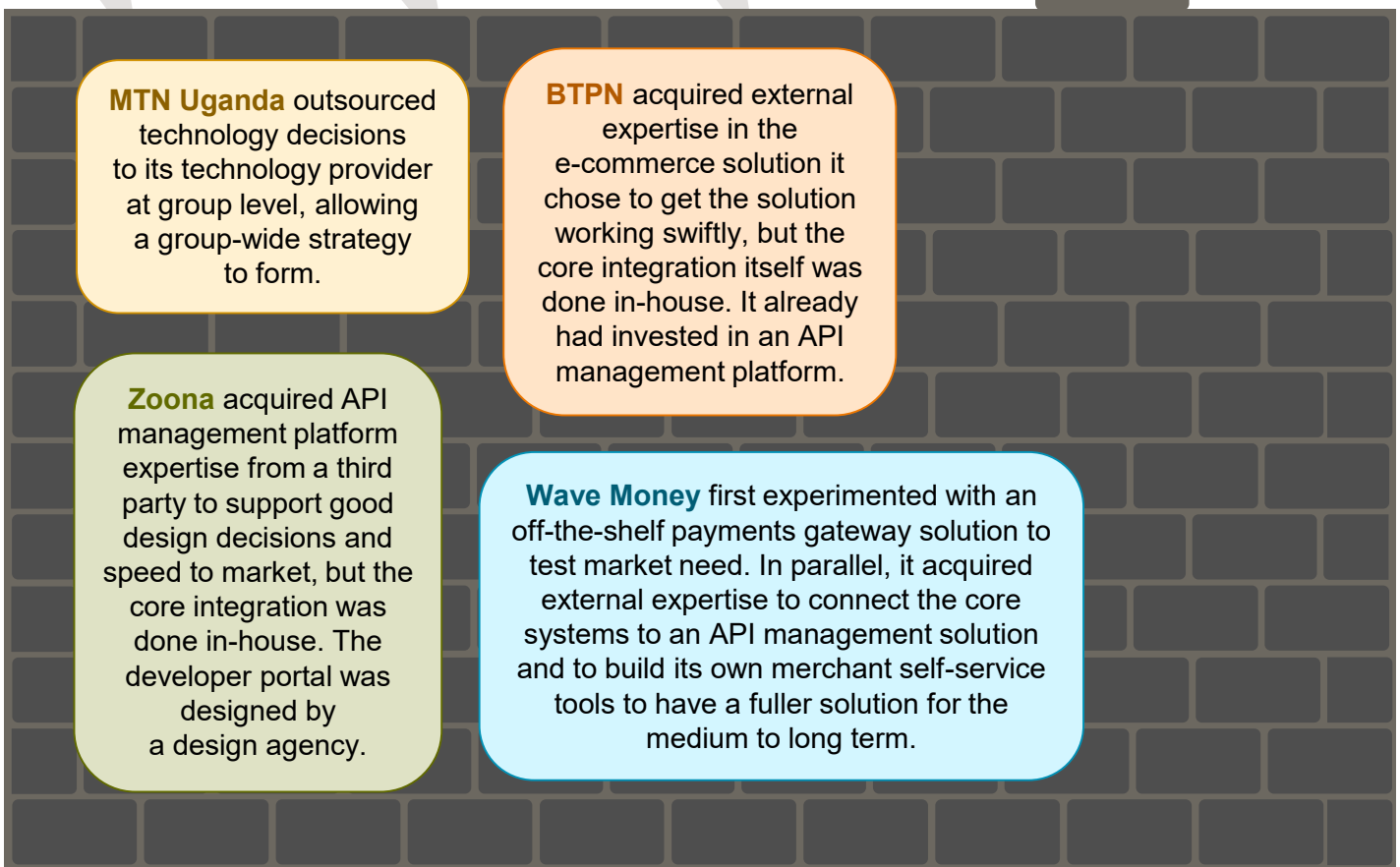
Partners asked themselves

Does the team have the right skill set?

Is support needed from our current vendors?

Do we need new external support?

All of our partners recognized in-house capability gaps and used external support to help fill that gap.



MTN Uganda outsourced technology decisions to its technology provider at group level, allowing a group-wide strategy to form.

BTPN acquired external expertise in the e-commerce solution it chose to get the solution working swiftly, but the core integration itself was done in-house. It already had invested in an API management platform.

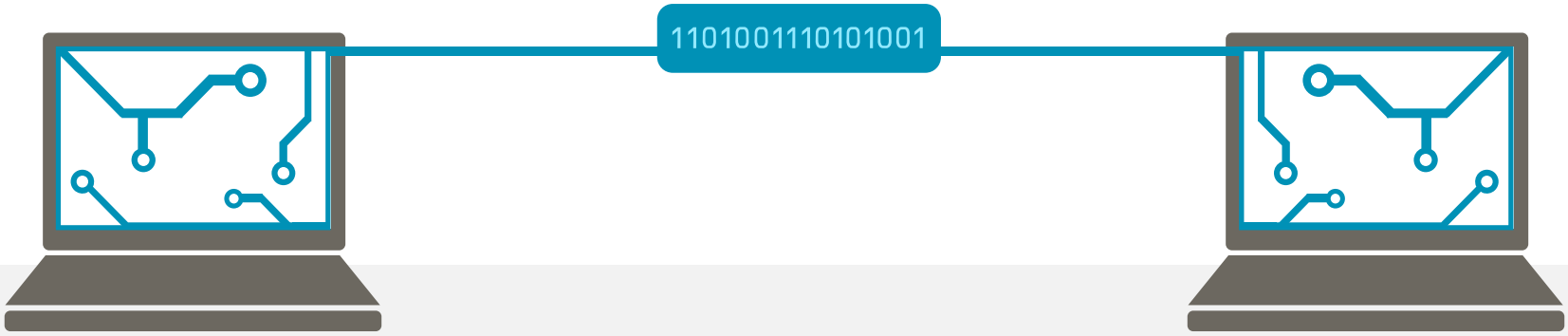
Zoona acquired API management platform expertise from a third party to support good design decisions and speed to market, but the core integration was done in-house. The developer portal was designed by a design agency.

Wave Money first experimented with an off-the-shelf payments gateway solution to test market need. In parallel, it acquired external expertise to connect the core systems to an API management solution and to build its own merchant self-service tools to have a fuller solution for the medium to long term.

© CGAP 2019

Should I adopt API standards?

DFS providers are responsible for storing data and moving money on behalf of customers. Standards around data and security help to ensure risks are minimized.



Simple API definition: The ability of computer systems or software to exchange and make use of information.

The reality of what is expected: The ability to automatically interpret information exchanged in a meaningful, timely, and accurate way to produce useful results as defined by the end users of two or more systems.

Standards describe what information should look like and how it should be interpreted when several parties wish to share information. Standards help the receiving party use the information correctly. If a standard isn't implemented, the business must explicitly define and document details.

Using standards can simplify this burden. Standards allow businesses to create solutions that are quickly interoperable and require minimum effort on training and knowledge sharing.

Standards make good business sense

There is a lot of merit in adopting standards that already have been well-tested and adopted by developers. For example, in India UPI standards adopted by providers enabled the fast spread of digital payments by Google, Amazon, and Facebook/WhatsApp.

Removing payments fragmentation created by the lack of standards is the business model of many payment gateways, switches, and aggregators. They make the situation less complex by removing the fragmentation, for a fee.

As of 2018, Stripe's $20 billion valuation is based on its business model of making payments as simple and standardized as possible via APIs globally. It has been instrumental in the adoption of new standards linked to PSD2 by small entrepreneurs.

What if API standards haven't been widely adopted yet?

Factors such as industry-wide acceptance, global use, and availability of required documentation can help determine whether to adopt a particular standard. Many of our partners are operating in markets where there is no widely adopted standard.

However, standards often are based on underlying design principles that can be used in the absence of a widely adopted standard. Here are 3 examples:

GDPR is formed from 6 privacy-by-design principles.

There are various payments schemes based on real-time push payments principles.

PSD2 regulations are based on open banking security principles.

Example: Leading the Charge

Starling Bank in the United Kingdom had an API-led strategy to deliver the best of fintech solutions to its customer base. From the outset, it used best practice security and hosting standards as part of building its bank technology, and it hired people from Silicon Valley companies like Xero and PayPal to build the platform.

If Starling Bank had waited for PSD2 standards to emerge, it would have lost its early adopter position and its ability to use its direct experience to influence standards setting.

It later modified its APIs and processes to comply with the PSD2 standard, which was not a complicated task as it already had been built to good privacy-by-design principles.

Source: https://www.starlingbank.com/blog/an-update-on-our-api/; https://www.starlingbank.com/blog/changing-the-way-third-party-data-is-shared/; https://www.starlingbank.com/blog/explaining-psd2-without-tlas-tough/ .

What security standards should I adopt?

An open API security architecture removes overly burdensome and costly requirements to establish a secure connection. Our partners needed to consider how information security standards and data protection policies would be affected by moving from a secure direct connection between third-party and DFS provider systems to an open API security architecture based on new standards using the internet.

Authentication (who you are) is used to determine the identity of a developer's application.

Authorization (what you can do) is used to determine what resources the identified developer has access to (e.g., which APIs can be called and which financial accounts and data the developer can access).

Security standards such as Developer API Keys for authentication and OAuth 2.0 for authorization allow open APIs to become a reality. Secure APIs are needed to protect end customers, manage consent, and develop a safe environment for a digital economy. A detailed description of security standards to consider for each of these elements is described "Finance-as-a-Service: API Playbook." Qualified experts can help you determine an up-to-date security architecture.

All of our partners chose to use developer API keys for authentication of third parties and JSON Web Tokens (JWT) for authorization via an industry-standard API management platform. MTN uses OAuth2.0, a security standard for the process that goes on behind the scenes to facilitate secure handling of consent.

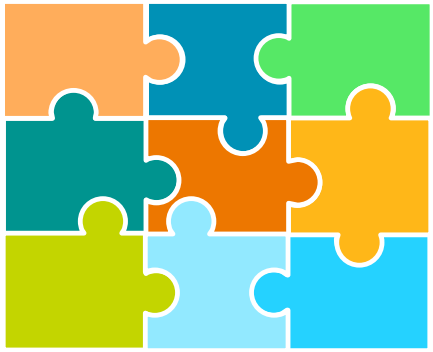
All partners used HTTPS to ensure all data were encrypted as data travelled on the Internet.

3. API technology building blocks

This section covers the key components DFS providers need such as the Developer Portal and Sandbox. Start here if you want some terminology explainers.

CGAP

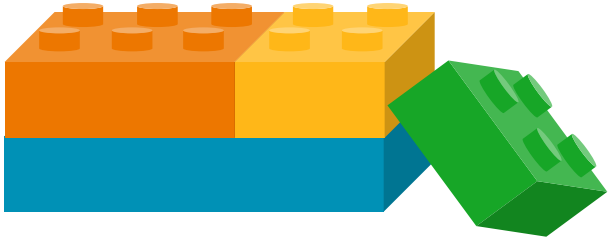
What is an open API? How does it differ from traditional integrations?



JIGSAW

Integrations: Highly customized, like designing a jigsaw puzzle

- The DFS provider chooses which partners to work with based on a justified business case.
- The DFS provider and the third party need to expend significant effort across several departments to build, test, and launch a project.



BUILDING BLOCKS

Open APIs: Like creating with toy building blocks

- The DFS provider presents the same building block options to all interested third parties who choose an option and develop against it.
- Focus is on as much self-service activity as possible, with DFS providers investing time and effort when it adds value, e.g., quality assurance.

CGAP

Source: "Great APIs Are Like Lego Bricks," Art Anthony, 27 April 2017, https://nordicapis.com/great-apis-like-lego-bricks/.

© CGAP 2019

Open API technology building blocks

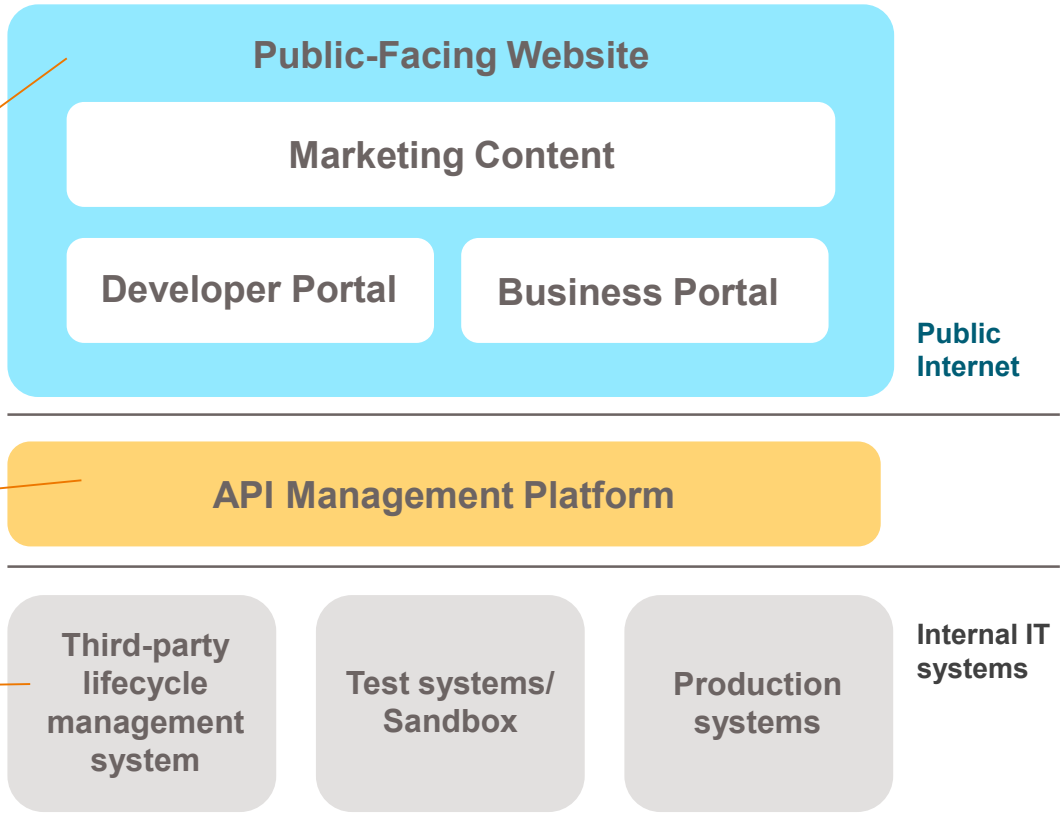
Four areas enable self-service on top of existing technology systems and are important in transitioning from integrations to open APIs.

1. Public-facing website: The simplest way to provide information is to create a website, often called the developer portal.

The business portal and developer portal may be two separate websites, or they may have a common landing page.

2. API management platform: This allows APIs to be securely exposed via the internet without needing a secure direct connection.

3. Third-party lifecycle management system: This usually is a new component that helps the DFS provider digitally manage third parties.



4. Sandbox: Beyond simple experimentation based on reference APIs, developers want to know their tests mirror real behavior on the live system. This needs to be designed because it is not included in an API management platform. DFS providers need to provide a Sandbox. This is most useful to developers when it simulates behavior in a production system that has an identical security model as the production environment.

© CGAP 2019

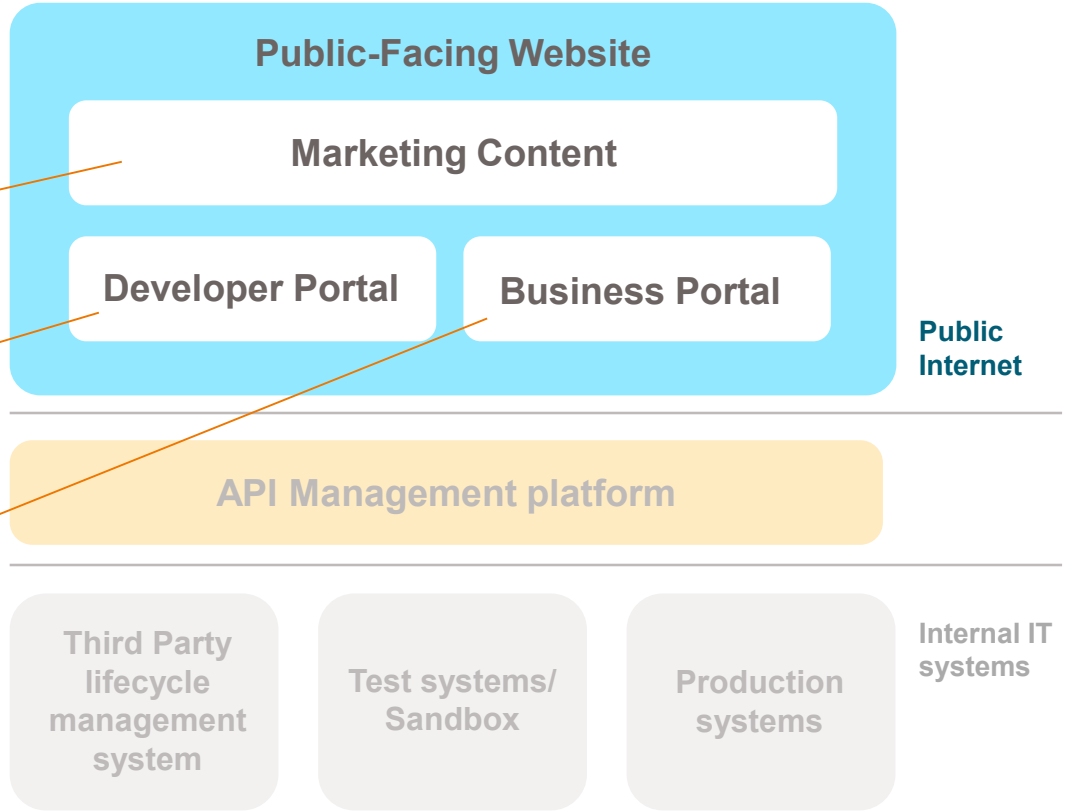
1.The public-facing website digitizes as many business processes as possible with third parties

The website (developer portal) has different content before and after login.

Marketing content helps third parties understand the value proposition before they invest resources.

Developers expect support to help them learn, onboard, and test in detail, from “just playing” to going live.

Third-party business stakeholders expect support systems to help them understand what they are paying for and what they can expect, and manage the legal and financial aspects of the relationship.



The website content often is managed via an off-the-shelf content management system such as Drupal, Joomla, or Wordpress connected to the API management platform, as this allows for easy iteration of the content.

© CGAP 2019

Questions the developer portal needs to answer

These features can be built out over time, depending on budget and team capacity.
Prioritize minimum viable product (MVP) and improve over time.

QUESTION FROM THIRD PARTY	FEATURE	MVP	BETTER	FULL
What is this?	Landing pages (marketing content)	x	x	x
How do I get started?	Tutorials	x	x	x
Do I know all the details?	API reference and basic sandbox	x	x	x
How do I get access?	Self-service sign-up and API key for sandbox	x	x	x
Can I trust this API?	Terms and conditions available online	x	x	x
How can I reach you?	Support contact details	x	x	x
How can I go live?	UAT* sandbox access and automated go-live process		x	x
Is somebody still working on this API?	Blog, community presence		x	x
How can I set up a business account?	Self-service business account application and document upload		x	x
How do I use your API in my app?	SDKs,† use case examples, or quotes/mini case studies		x	x
What do I need to understand?	Concept explainers: e.g., how security works, how commissions are calculated, or how balance updates work			x
How do I create a specific use case?	Guides			x
Can I afford this API?	Pricing standardization online			x

CGAP

*User acceptance testing; †Software development kit

© CGAP 2019

Developer portal content in detail

Use this checklist to help you think through what third parties will value; it will form the basis of a business requirements roadmap.

PHASE	FEATURE	FOR BUSINESS	FOR DEVELOPER
Throughout	Get Support—Community Support (hosted or, e.g., Slack/Whatsapp/Telegram)		x
	Get Support—Helpdesk System (e.g., Intercom, Zendesk, Hubspot)	x	
1a. Awareness: Bring clarity to visitors about what the API does and the opportunities it offers.	Value Proposition Marketing Content	x	
	Read Testimonials and Real-World Stories	x	
	Find Details on Use Cases	x	
	Standardized Pricing information	x	
	Get-Started Guides		x
	Full API Reference		x
	Code Examples		x
	Basic Sandbox to See API Responses		x
1b. Consideration: Ensure visitors can explore and experiment with integrating APIs and help them decide.	Terms of Service	x	
	Showcase Blogs	x	x
	Business FAQs	x	
	Technical FAQs		x
	Catalog of Certified Developers/Partners	x	
	Developer Sign-Up Form		x
	Information on Security/Authentication		x
	Tutorials and Recipes		x
	API Versioning Details		x
	Information on Errors		x
	Plugins/Widgets/SDKs		x
	Webhook Endpoint Management Set-up		x
	UAT System Developer Key Access		x
	Better Sandbox Showcasing Full Security and Simulating Live Environment		x
2. Onboarding: Simplify and automate process as much as feasible	Information on Business Application Process	x	
	Business Application Process Form	x	
	Business Documentation Upload Form	x	
	Information on Go-Live Process		x
	Submit UAT Test Results		x
	CONSENT—Verify Developer Access (e.g., 2FA process)	x	x
3. Use: Easy access to performance and billing data	Live System Developer Key Access (CONSENT)		x
	API Status Information		x
	Information on API Performance	x	x
	Billing/Settlement Data	x	x
4. Growth: Innovation and revenue opportunity support	Beta Access to New APIs	x	x
	Business Analytics	x	
	Learning Management (e.g., Certification/Training Management)		x

© CGAP 2019

2. API management platform

An API management platform robustly protects core systems.

The platform sits in line with incoming traffic and enforces API policies, including key validation, quota management, authorization, and access control, before passing the request to the underlying core DFS service. Many of these components are available individually via open source but often are packaged together commercially into an API management platform. Cloud providers offer several of these elements as part of their basic service.

FEATURE	DESCRIPTION
API Gateway	An API gateway funnels API requests to the right core systems. It is the core piece of infrastructure that enforces API security. Unlike traditional firewalls, API security requires analyzing messages, tokens, and parameters in an intelligent way. Its main benefit is moving security from the application to your organizational infrastructure. The API gateway first checks authorization. It then checks parameters and the content sent by authorized users. Next, it ensures that when logs are written, they're redacted, customer data are not in the logs, and logs do not get written into storage. And it accomplishes these steps in the proper order.
Traffic Management	The traffic management component limits the number of queries for each developer account per second or per day. This is a risk management tool. It stops developer solutions from making more requests than the underlying service can handle and creating what is effectively a denial-of-services attack, whether intentional or not.
Data Caching	The data caching component remembers if a developer's service recently asked for data. This limits the number of repeat requests and improves overall performance.
API Use Monitoring	API use monitoring helps teams understand how the service is performing technically and detects issues early. This provides insights into traffic patterns.
API Use Billing	Some API management platforms have API-centric billing mechanisms based on API use per developer.
Developer Key Management	A developer key is the "key" to entry to the service, like a password. The key authentication module ensures that incoming API requests are from a uniquely identified and authorized developer application.
API Design and Versioning	Beyond its operational role, many API management platforms help with API governance: it enables API providers to design APIs, use policies, deploy APIs, and manage version control.

CGAP

Source: "Why API Management," apigee, https://apigee.com/about/cp/why-api-management.

© CGAP 2019

3. Third-Party lifecycle management

Providers will need a system to provide back-office support. The system should include the following functionality:

- An understanding of partners in the sales funnel and progress in each phase
- Digital responses to questions
- Ability to upload and later retrieve digital KYC documentation and signed contracts
- Ability to manage and later retrieve go-live approvals

SaaS customer relationship management solutions such as Zendesk or Intercom often are woven into the solution to ensure that third-party employees can direct queries to the right part of the business and use standard marketing tools to reach out to partners and monitor KPIs.

All automated processes will similarly need back-office logic and databases to manage partner status and API consent:

- E.g., business owners will authorize their chosen developer to access their account. Without this, the developer can't access the live systems. If done digitally, consent needs to be stored, checked, and revoked when requested.
- This happens in digital businesses even when financial interactions aren't involved. E.g., when you connect your Gmail account to an app on your phone, Google asks for your "consent" to allow the mail app on your phone to access your email and send email for you.

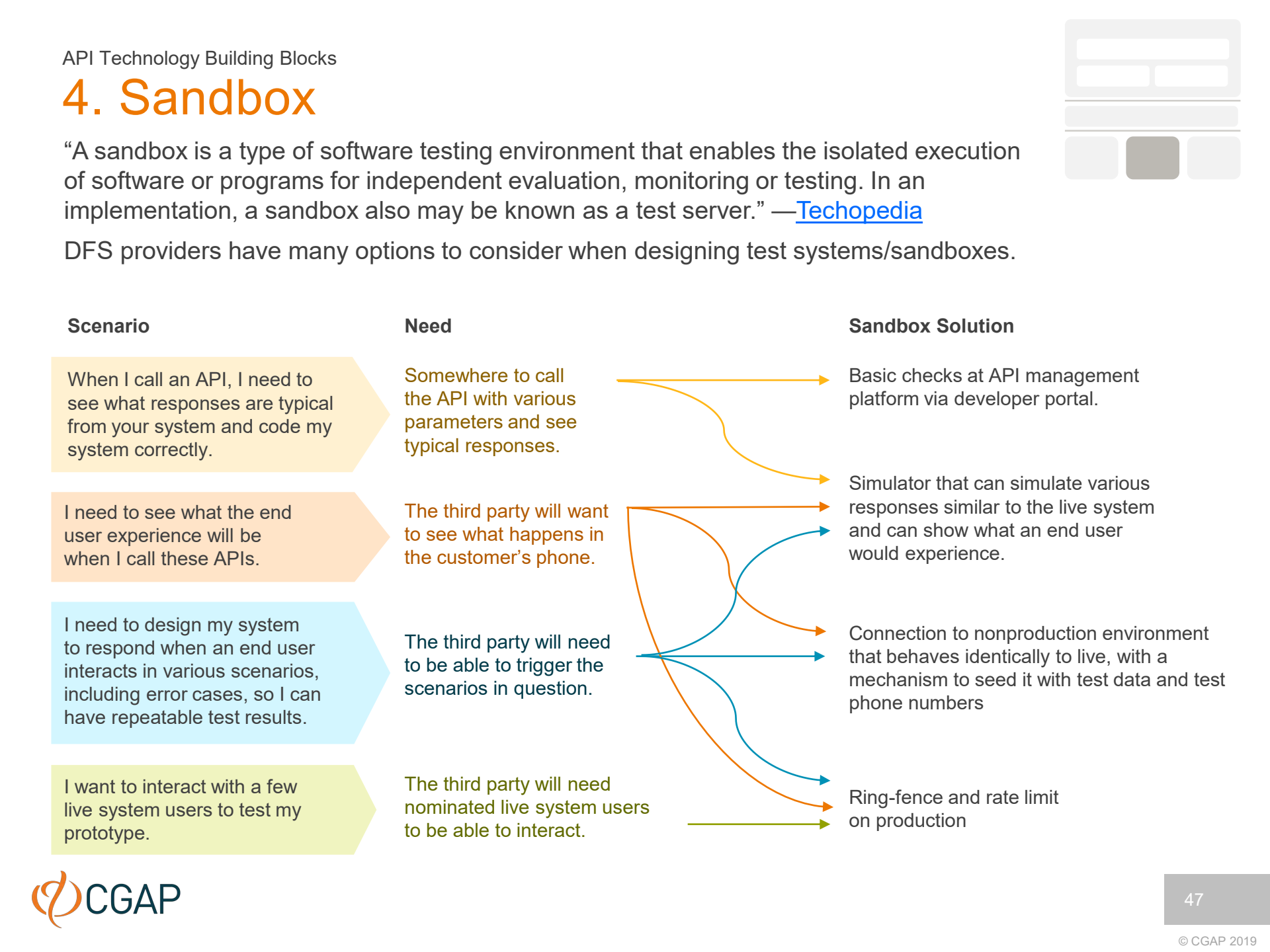
© CGAP 2019

4. Sandbox

"A sandbox is a type of software testing environment that enables the isolated execution of software or programs for independent evaluation, monitoring or testing. In an implementation, a sandbox also may be known as a test server." —Techopedia

DFS providers have many options to consider when designing test systems/sandboxes.

Scenario	Need	Sandbox Solution
When I call an API, I need to see what responses are typical from your system and code my system correctly.	Somewhere to call the API with various parameters and see typical responses.	Basic checks at API management platform via developer portal.
I need to see what the end user experience will be when I call these APIs.	The third party will want to see what happens in the customer's phone.	Simulator that can simulate various responses similar to the live system and can show what an end user would experience.
I need to design my system to respond when an end user interacts in various scenarios, including error cases, so I can have repeatable test results.	The third party will need to be able to trigger the scenarios in question.	Connection to nonproduction environment that behaves identically to live, with a mechanism to seed it with test data and test phone numbers
I want to interact with a few live system users to test my prototype.	The third party will need nominated live system users to be able to interact.	Ring-fence and rate limit on production



CGAP

© CGAP 2019

Example: Prototyping in the “real world”

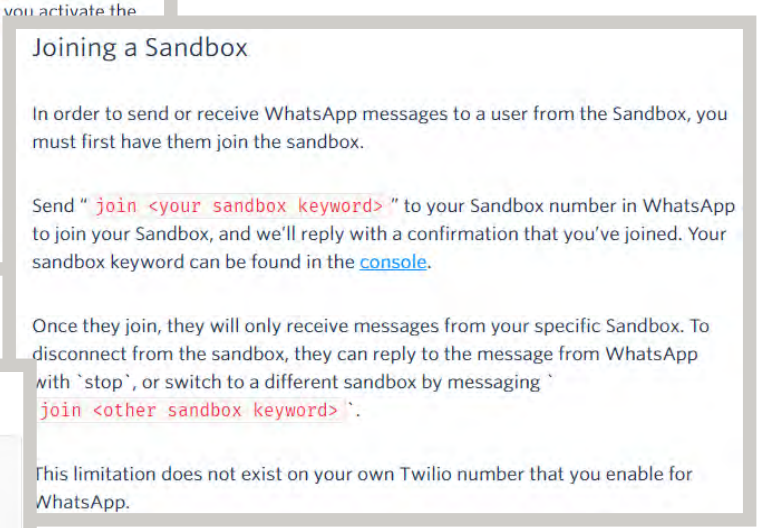
Twilio’s WhatsApp sandbox uses the live WhatsApp network.

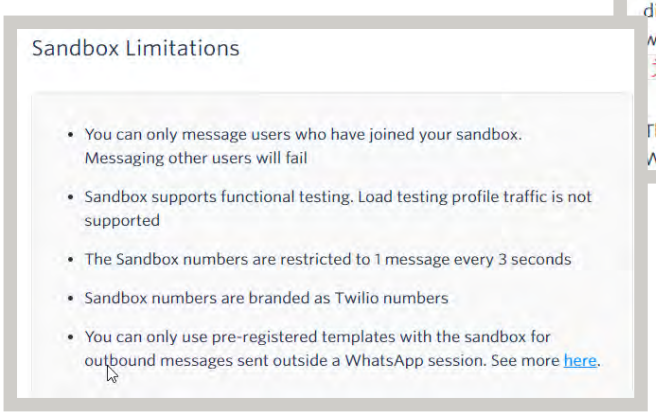
Cloud communications platform as a service company.

Twilio understands that developers need to test actual platform behavior as quickly as possible. The easiest way to do this is to allow the developer to interact with real WhatsApp end users.

Twilio’s WhatsApp sandbox enables end users to use their personal WhatsApp account or test SIMs and phones to interact with the developer solution.

The live system sandbox is protected by allowing only the developer’s software to interact with opted-in WhatsApp users and by throttling the volume of messages the developer code can send.





Source: https://www.twilio.com/docs/sms/whatsapp/api#twilio-sandbox-for-whatsapp.

© CGAP 2019

Resources

CGAP

Resources

Developer Portals
Pronovix blog on doing developer portals: https://pronovix.com/articles
CGAP API dashboard for examples of APIs: https://cgap.apidashboard.io/

Discoverability and Platform Thinking
Starling marketplace blogs: https://www.starlingbank.com/marketplace/
Wechat Platform explained: https://youtu.be/j3OOS-3oU8k
https://www.cgap.org/blog/series/platform-economy-what-it-means-financial-inclusion
https://www.cgap.org/blog/chinas-super-platforms-impact-question
https://www.cgap.org/blog/super-platforms-africa-not-if-when
Wechat discoverability: https://www.bloomberg.com/opinion/articles/2019-01-11/tencent-s-mini-programs-could-open-up-wechat-for-business-use

API Education
API Academy: https://apiacademy.co/resources/
JSON Web Tokens: https://jwt.io/introduction/
Programmable Web: https://www.programmableweb.com/api-university/what-are-apis-and-how-do-they-work

Gartner reports for API Management solutions:
- https://www.gartner.com/en/documents/3873383
- https://www.gartner.com/en/documents/3956412
- https://www.gartner.com/en/documents/3947297
- https://www.gartner.com/en/documents/3913711

Standards
MAS API Playbook: https://abs.org.sg/docs/library/abs-api-playbook.pdf
PSD2 explained: https://transferwise.com/gb/blog/what-is-psd2
Technical standards on strong customer authentication and secure communication: https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2
Open Banking: https://standards.openbanking.org.uk/
Example of how APIs support GDPR: https://www.rocketsoftware.com/product-categories/compliance-solutions/general-data-protection-regulation-gdpr-rocket-api
GSMA Mobile Money standard: https://developer.mobilemoneyapi.io/
GSMA cybersecurity framework: https://www.gsma.com/mobilefordevelopment/blog/cybersecurity-a-governance-framework-for-mobile-money-providers/
Mojaloop API standard: https://mojaloop.io/documentation/api/mojaloop-api-specification.html

© CGAP 2019

CGAP

www.cgap.org