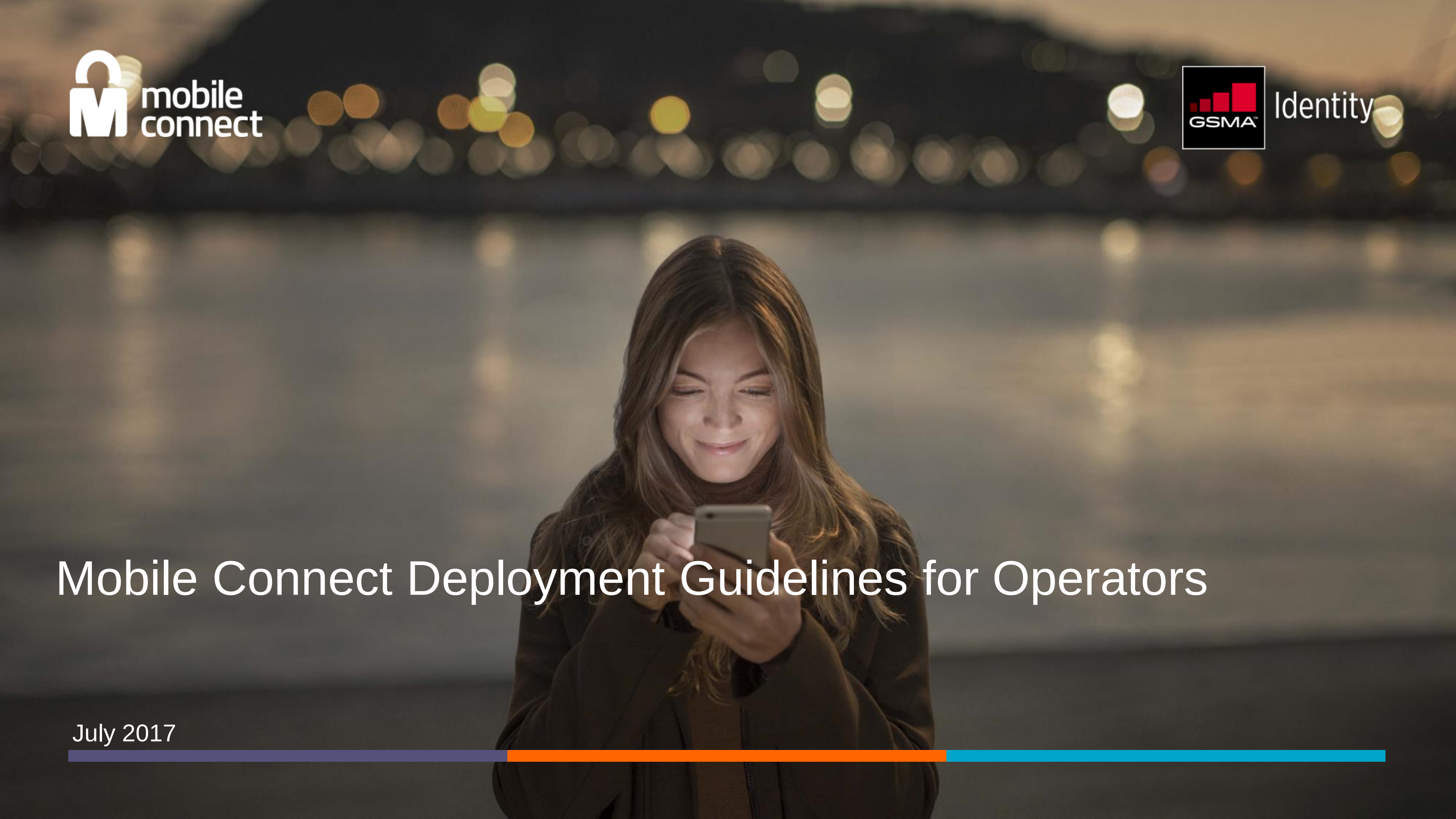


Mobile Connect Deployment Guidelines for Operators

July 2017

Deployment stages and activities

Mobile Connect deployment guidelines for operators

Deployment stages and activities

Planning

- Products
- Authenticators
- ID Gateway
- API Exchange
- Request validator
- Analytics
- Ts&Cs
- User registration
- Service mark
- User flows
- User experience
- Regulatory analysis
- Privacy principles
- Resources

Technical Implementation

- Implementation
- API compatibility testing
- Performance testing
- End-to-end testing
- UX

Pre-launch

- SP identification
- SP contracts
- SP billing & reconciliation
- Pricing model
- GSMA SP outreach
- End user and SP support
- Marketing campaign
- PR
- Digital content
- Consumer incentivisation

Launch

- Public launch

Operational/BAU

- Analytics
- Reporting

Planning stage: Selecting Mobile Connect products

Mobile Connect deployment guidelines for operators

mobile connect

Planning: Which Mobile Connect products to deploy?

Authentication	A simple, safe end user authentication solution on a global scale	authenticate	authenticate plus	
Authorisation	Authenticate as well as authorise requests directly from mobile	authorise	authorise plus	
Identity	End user consent to share personal attributes data	phone number	national ID	sign-up
Attributes	Mobile subscriber ID verification for digital services	account takeover protection	KYC match	verified MSISDN

Product category: Authentication

Mobile Connect Authentication offers a simple and globally ubiquitous log-in mechanism.

authenticate

Mobile Connect Authenticate provides a mechanism for authenticating the user based on their possession of mobile phone i.e. something the user has; as such, Mobile Connect Authenticate provides a single factor level of assurance (LoA2).

authenticate plus

Mobile Connect Authenticate Plus challenge the user to enter the Mobile Connect PIN on their mobile, or to authenticate via a biometric; possession of the mobile phone and either the PIN or biometric resulting in a two-factor authentication (LoA3).

Product Category: Authorisation

Mobile Connect Authorisation offers contextual authentication with a Yes/No option for users to authorise requests on their mobile phone.

authorise

Mobile Connect Authorise provides a mechanism to display specific request on the end user's mobile phone for approval. The end user approves or rejects the request and the response is relayed back to the service provider

authorise plus

Mobile Connect Authorise Plus extends Mobile Connect Authorise by requiring explicit user authentication via a PIN or biometric prior to the user approving the authorisation request

Product Category: Identity

Mobile Connect Identity helps end users engage with digital services quickly and efficiently, share data when they want to, and assert their identity when needed.

phone number

Mobile Connect Phone Number enables the end user to give their consent for their operator to share the phone number with the requesting service provider

sign-up

Mobile Connect Sign-up enables the end user to give their consent for their operator to share core information about them (first name/last name, street address, postal code, country) with the requesting service provider

national ID

Mobile Connect National ID enables the end user to consent to sharing their core ID information in accordance with local legislation & regulations. This service enables the requesting service provider to access the user’s first name/last name, date of birth, and national identifier

mobile connect

Product Category: Attributes

Mobile Connect Attributes services utilise device and network information for ID verification and fraud prevention.

KYC match

Mobile Connect KYC Match provides a comparison of the user’s name and address relative to the subscriber information held by the mobile network operator

account takeover protection

Mobile Connect Account Takeover Protection provides information on the pairing between a user’s mobile phone account and their device (i.e. last SIM change date and active call divert status) for fraud prevention

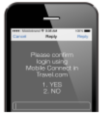
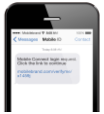
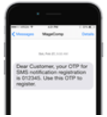
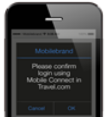
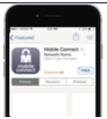
verified MSISDN

Mobile Connect Verified MSISDN verifies the phone number associated with a mobile device through which a user is accessing an SP’s service

Planning stage: Selecting authenticators

Mobile Connect deployment guidelines for operators

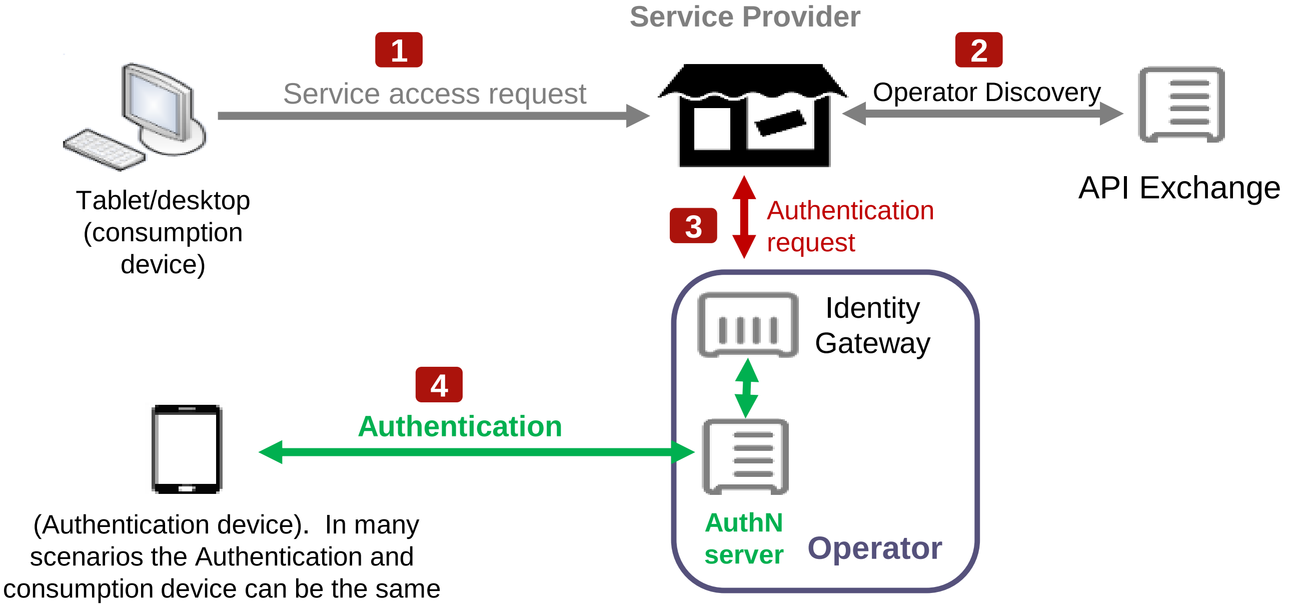
Selecting authenticators

		Pros	Cons
USSD	 Please confirm login using Mobile Connect in Travel.com 1. YES 2. NO	• Works on all phones • Doesn't require data connections • Secure channel	• Requires user input • Can take time loading • Displays differently on different devices
SMS/URL	 Mobile Connect login request. Click the link to continue mobilebrand.com/verify/e/x1498j	• No user input required • Works consistently across enabled devices	• Low security • Requires data connection • Data charge may discourage users
SMS/OTP	 Dear Customer, your OTP for SMS notification registration is 012345. Use this OTP to register.	• Works consistently across enabled devices • Works on every single phone	• Not secure • OTP requires User Input • 8 step process
SIM Applet	 Mobilebrand Please confirm login using Mobile Connect in Travel.com Cancel OK	• Super quick and secure (esp. for LoA3)	• Limited text strings for UX display • High investment to roll out
Smart Phone App	 Mobile Connect FREE	• Very smooth UX as eliminates call times and processes	• Only available for smartphones

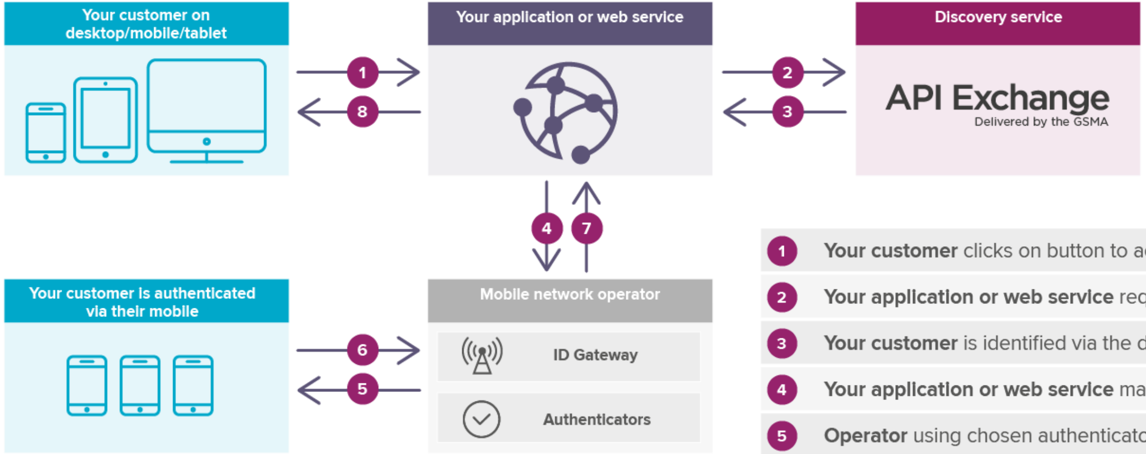
Planning Stage: ID Gateway

Mobile Connect deployment guidelines for operators

Identity Gateway (ID GW)



Identity Gateway (ID GW)



Your customer on desktop/mobile/tablet
Your application or web service
Discovery service
API Exchange
Delivered by the GSMA
1
8
2
3
4
7
Your customer is authenticated via their mobile
Mobile network operator
ID Gateway
Authenticators
6
5

1 **Your customer** clicks on button to access service

2 **Your application or web service** requests customer's operator from the discovery service

3 **Your customer** is identified via the discovery service

4 **Your application or web service** makes a request for authentication using OpenID with Mobile Connect profile

5 **Operator** using chosen authenticator seeks authenticate request

6 **Your customer** follows instructions on their mobile to enable authentication

7 **PCR** identifying a specific end user is returned

8 **Access granted**

Planning: ID Gateway

Operators may choose an in-house ID gateway deployment or may partner with an external vendor to handle the implementation. Referred to as “Mobile Connect Accelerator” (MCX).

MCX is a cloud-based managed service, designed to help operators implement Mobile Connect in an easy and fast manner. The service circumvents the need for operators to spend time and resources finding appropriate compliant platforms by themselves.

Details about MCX providers can be found here: http://www.gsma.com/personaldata/mobile-connect-accelerator-mcx

Operators exposing the Mobile Connect APIs should follow the Mobile Connect technical specifications found on InfoCentre2.

Compliance with the Mobile Connect technical specifications can be certified using the Mobile Connect Test Suite Portal.

Planning stage: API Exchange

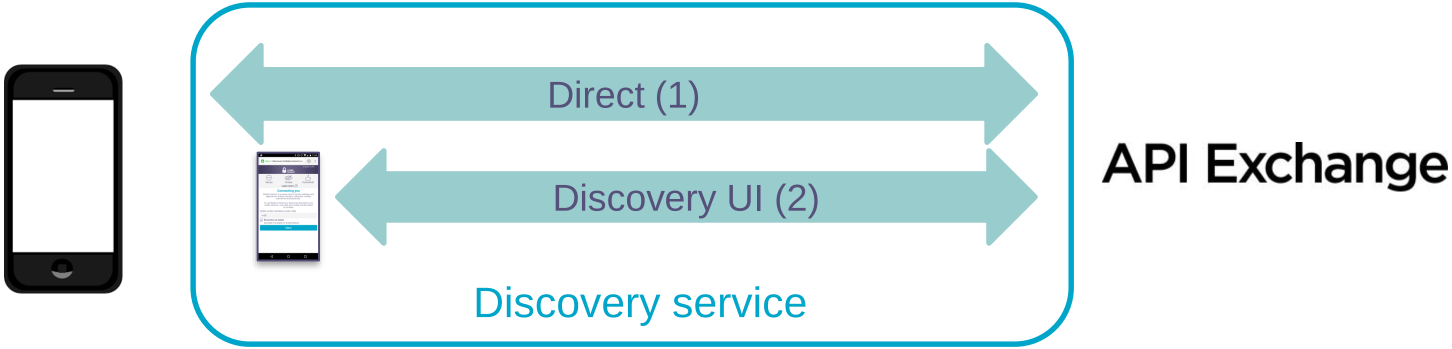
Mobile Connect deployment guidelines for operators

Planning: API Exchange?

The API Exchange offers a federated discovery service that allows a third party to discover the home mobile operator of any mobile phone.

The discovery service can be completed without end user interaction (1).

If end user interaction is required, then the discovery user interface (2) is displayed.



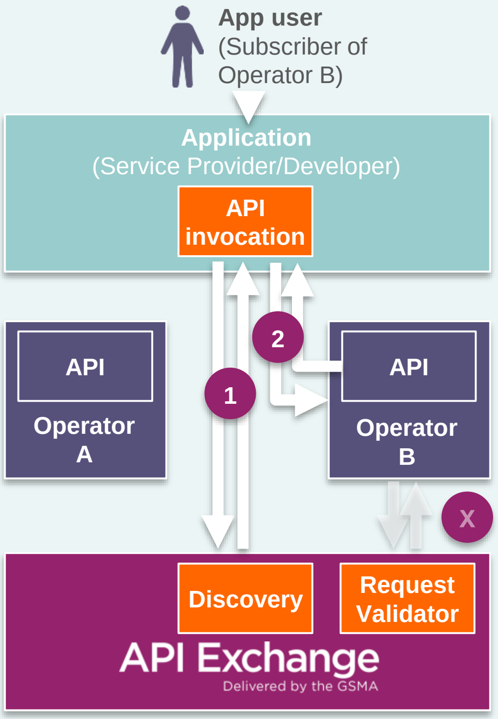
Direct (1)

Discovery UI (2)

Discovery service

API Exchange

Planning: API Exchange by GSMA



Flow

1 Application calls global **"Discovery"** capability to determine to which operator a subscriber / user of the application belongs, leveraging IP address, MSISDN, MCC/MNC from SIM …

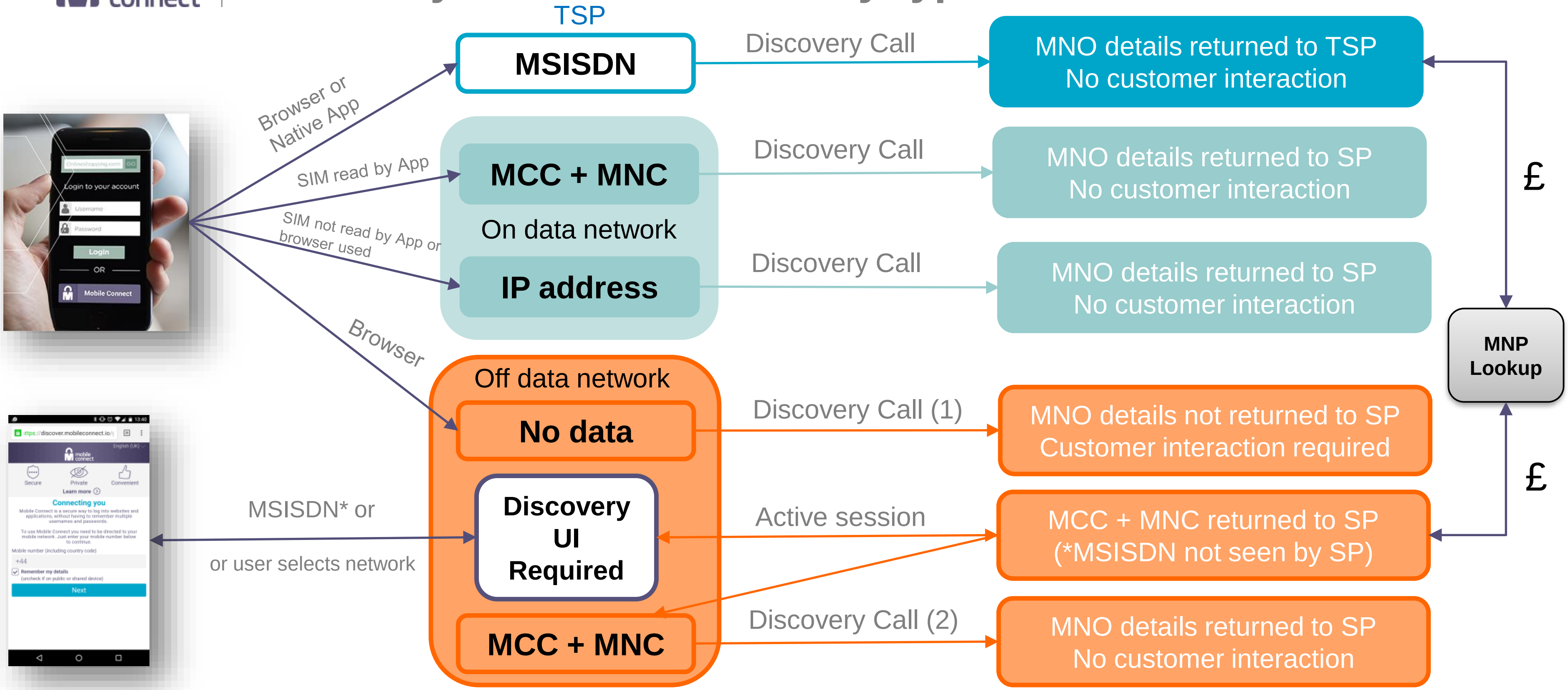
Return: Operator B details, API exposure endpoint address and access credentials

2 Application calls **"API"** of discovered, Operator B

X (optional): Operator B calls **"Request Validator"** to validate API access credentials and details of invoking application/ developer (*)

* If operator does not want to use "Request Validator" they can instead implement an application whitelist

Discovery service – Discovery types



TSP

MSISDN

Browser or Native App

SIM read by App

SIM not read by App or browser used

Browser

MCC + MNC

On data network

IP address

Off data network

No data

Discovery UI Required

MCC + MNC

Discovery Call

Discovery Call

Discovery Call

Discovery Call (1)

Active session

Discovery Call (2)

MSISDN* or

or user selects network

MNO details returned to TSP
No customer interaction

MNO details returned to SP
No customer interaction

MNO details returned to SP
No customer interaction

MNO details not returned to SP
Customer interaction required

MCC + MNC returned to SP
(*MSISDN not seen by SP)

MNO details returned to SP
No customer interaction

MNP Lookup

£

£

ittps://discover.mobileconnect.io/

English (UK)

Secure Private Convenient

Learn more

Connecting you

Mobile Connect is a secure way to log into websites and applications, without having to remember multiple usernames and passwords.

To use Mobile Connect you need to be directed to your mobile network. Just enter your mobile number below to continue.

Mobile number (including country code): +44

☑ Remember my details
(uncheck if on public or shared device)

Next

API Exchange contracting

The API Exchange service allows operators to federate their Mobile Connect APIs in order to enable a service provider using Mobile Connect to reach any mobile user without having to connect directly with each operator. The API Exchange service will be offered at different service tiers to accommodate for different business needs, summarised below:

Service tier 1 & 2 – Intended for Pilots (**Tier 1**) and limited commercial service (**Tier 2**) with up to 30 million API calls free of charge but reduced support and guarantees.

Service **Tier 3** – Designed for a commercial service with agreed availability levels and improved support SLA's. Priced based on transaction bundles.

Planning stage: Analytics

Mobile Connect deployment guidelines for operators

Planning: Analytics

GSMA recommendations to operators:

- Analytics must be in place across all the deployed components. It is essential that all incidents (technical activity) is logged and user traffic monitored.
- Analytics must be included in initial contracts with technical vendors.

GSMA collects and aggregates high-level metrics on a monthly basis from all operators globally to measure the success of Mobile Connect

- # registered and monthly active users
- # successful and unsuccessful transactions (in some markets, detailed reasons for failures)
- # of applications (with name/sector as much as possible)

Data available related to the Discovery API:

- API calls per operator and per application
- Call successes/reasons for failure
- Latency, uptime, and other SLA metrics

Planning stage: T&Cs for Mobile Connect (Click-to-Accept)

Mobile Connect deployment guidelines for operators

Click-to-Accept: Operator proposition for a distribution channel to build scale

Distribution Agreement between GSMA and MNO

- Includes the consolidated **global SP T&Cs (v12)** as an Exhibit
- Only localisation is operator name and Address
- Operator specific terms are already in the SP terms
- SP is obligated to follow all Local laws and regulations

Supports a **limited proposition** initially (new functionality will come later):

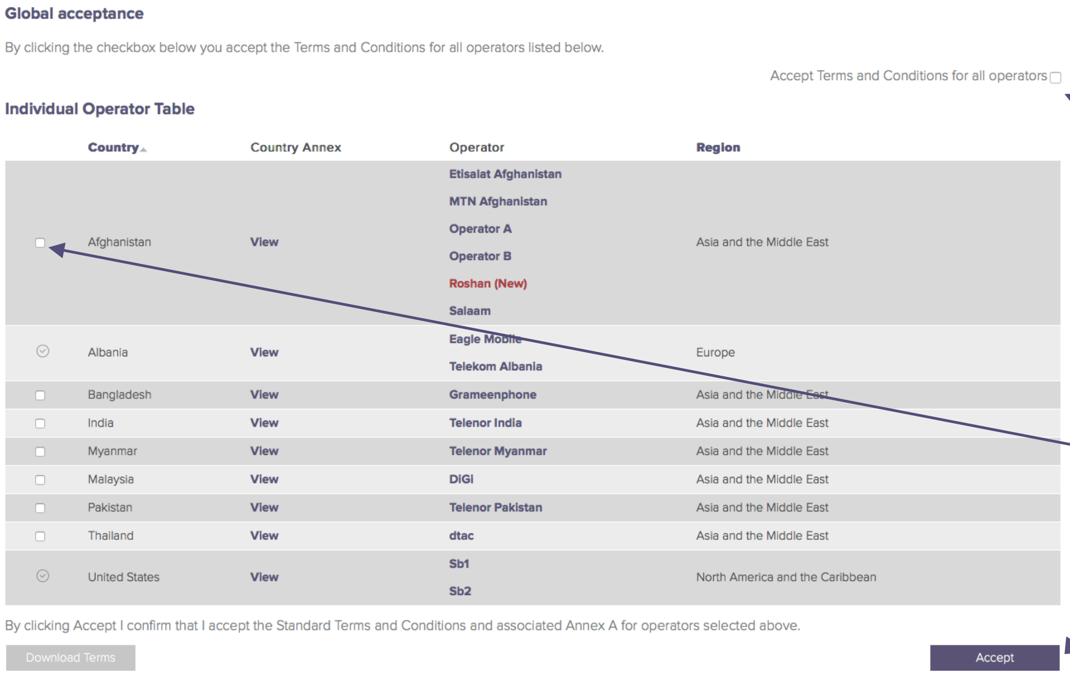
- Simple Authentication only (typically LoA2)
- Free services for developers (subject to fair usage limitations)

An **optional** channel to market for operators but not the only one

- Operators should progress with additional channels to market, such as reseller, aggregator, channel partners or directly through existing operator developer portals

Note: Operator can still say NO to an SP and blacklist application

Click-to-Accept: Simple and intuitive process for developers to contract with operators across multiple countries



Global acceptance

By clicking the checkbox below you accept the Terms and Conditions for all operators listed below.

Accept Terms and Conditions for all operators □

Individual Operator Table

	Country	Country Annex	Operator	Region
□	Afghanistan	View	Etisalat Afghanistan MTN Afghanistan Operator A Operator B Roshan (New) Salaam	Asia and the Middle East
✓	Albania	View	Eagle Mobile Telekom Albania	Europe
□	Bangladesh	View	Grameenphone	Asia and the Middle East
□	India	View	Telenor India	Asia and the Middle East
□	Myanmar	View	Telenor Myanmar	Asia and the Middle East
□	Malaysia	View	DiGi	Asia and the Middle East
□	Pakistan	View	Telenor Pakistan	Asia and the Middle East
□	Thailand	View	dtac	Asia and the Middle East
✓	United States	View	Sb1 Sb2	North America and the Caribbean

By clicking Accept I confirm that I accept the Standard Terms and Conditions and associated Annex A for operators selected above.

The developer can tick this box and then click Accept (below) to agree the standard T&Cs for all countries

The developer can tick one or many country boxes and then click Accept (below) to agree the standard T&Cs for the selected countries

To fully understand the Developer experience please go to https://developer.mobileconnect.io/

Click-to-Accept : Simple operator on boarding and ongoing support processes

Step 1	Step 2		Step 3	Step 4	Step 5
Operator Execute Distribution Agreement	**GSMA** Publish Operator Details	●	**Developer** Accept Operator T&Cs	**Developer** Promote App to live	**Operator** In Life Support
Return exhibit 1 Operator details as they will appear on the Portal and ongoing contact information	Notify Developers of new operator Notify Operator	Operator Onboarding Complete	Operator is notified by email Exchange is updated	Operator is notified by email to whitelist the App on their Network	Responding to support requests and commercial enquirers, as defined in Exhibit 1

Planning stage: User registration

Mobile Connect deployment guidelines for operators

Planning: User registration

MNOs should decide how to register the service end users (e.g. offline pre-registration; on-the-fly registration etc.). It is recommended to include Mobile Connect as a standard service (like SMS, voice) and add specific Mobile Connect Ts&Cs into existing end user contracts.

Increasingly operators are now pre-registering new users for Mobile Connect when they enter into a new contract.

Existing users are enrolled into Mobile Connect through the operators own internal services.

Others have an existing user base of similar services so no new registration is needed.

A few may still require their end users to sign up on the fly as they use Mobile Connect for the first time.

There is full focus on optimising this process so to keep the friction to a minimum while still ensuring that the end users are fully informed about the service.

User Registration: Mobile Connect T&Cs Handling

Options for user to accept T&Cs	UX Advantages	UX Disadvantages
Offline when customer signs or renews contract with their Operator	Frictionless yet transparent process with full explanation of user benefits & MC proposition when contract is purchased on premise.	For contract renewals, the process may be invisible to the user and doesn't guarantee awareness.
IN product flow as extra 1 time only screen for clear acceptance	Full transparency to user. Education that T&Cs are available to be read if required.	1-time only screen/step extends the authentication process as it requires explicit user action to accept. Can therefore be a drop-out point.
IN product flow as blurb hardcoded & pre-checked underneath MC-sign in button	Full transparency to user. Link to T&Cs that can be read if required. Doesn't require explicit user-action for acceptance & proof of acknowledgement.	Unlikely to be accepted on SP sites or requires higher investment of UX design to contextualise on an SP site by site basis.
T&Cs handled as part of a **pre opted-in process** accompanied by an opt-out sms/email/comms campaign	Frictionless yet transparent process with full explanation of user benefits & MC proposition. Can be used as one piece of a wider marketing campaign by MNO / SP on actions to safeguard end user digital identity.	No UX disadvantages however there may be legal, regulatory or compliance issues as to why this may not be permissible in specific countries.
SP includes MC T&C in their own general contract **T&Cs**	Frictionless, invisible process to user.	No UX disadvantages however operators may feel they have legal, regulatory or compliance "exposure" and require some audit method.

Planning stage: Service mark

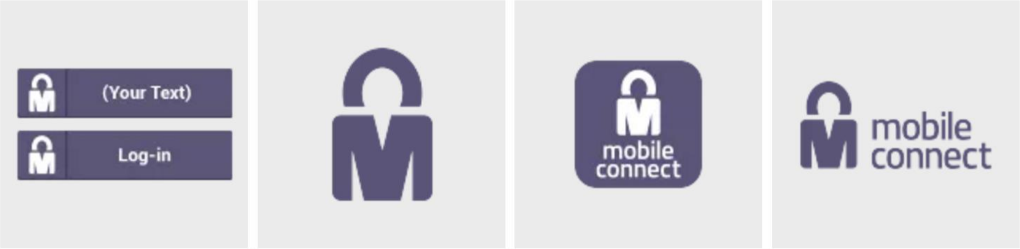
Mobile Connect deployment guidelines for operators

Uniting behind the Mobile Connect service mark

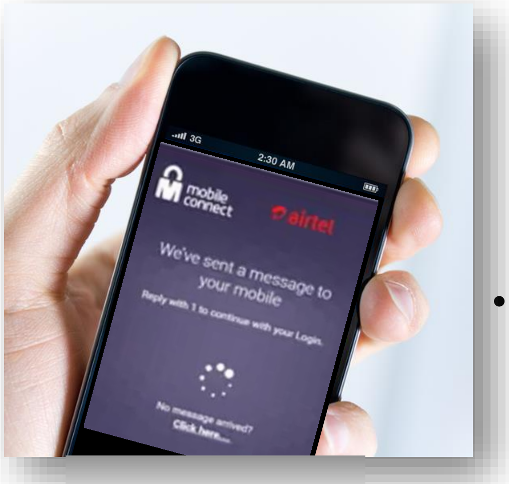
- The goal of the Mobile Industry and the GSMA is to make the Mobile Connect service mark the **single, trusted symbol for authentication** via a mobile phone. One that is recognised and trusted by consumers and service operators worldwide.

- **Unity is important**. If there are different names and identities for the service, it may create confusion amongst consumers and lack of trust amongst service operators. The more we can unite behind the Mobile Connect service mark, the faster it will be used and adopted.

- This is why the GSMA encourages all operators that are offering a compliant authentication service to adopt the existing Mobile Connect name and service mark guidelines.



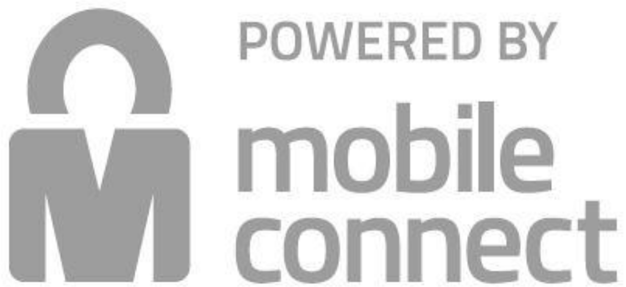
Mobile Connect service mark: A pragmatic approach


3G
2:30 AM
mobile connect
airtel
We've sent a message to your mobile
Reply with 1 to continue with your Login.
No message arrived?
Click here...

- In some instances, operators may wish to use Mobile Connect in conjunction with an existing identity service name. For example, when the existing brand pre-dates the launch of Mobile Connect and is already established as a mobile phone authentication service in that country or region.

- Whist the GSMA's preference is for the Mobile Connect name and service mark to used for the reasons already stated, in these circumstances, we encourage operators to at least *introduce* the Mobile Connect name and/or button.

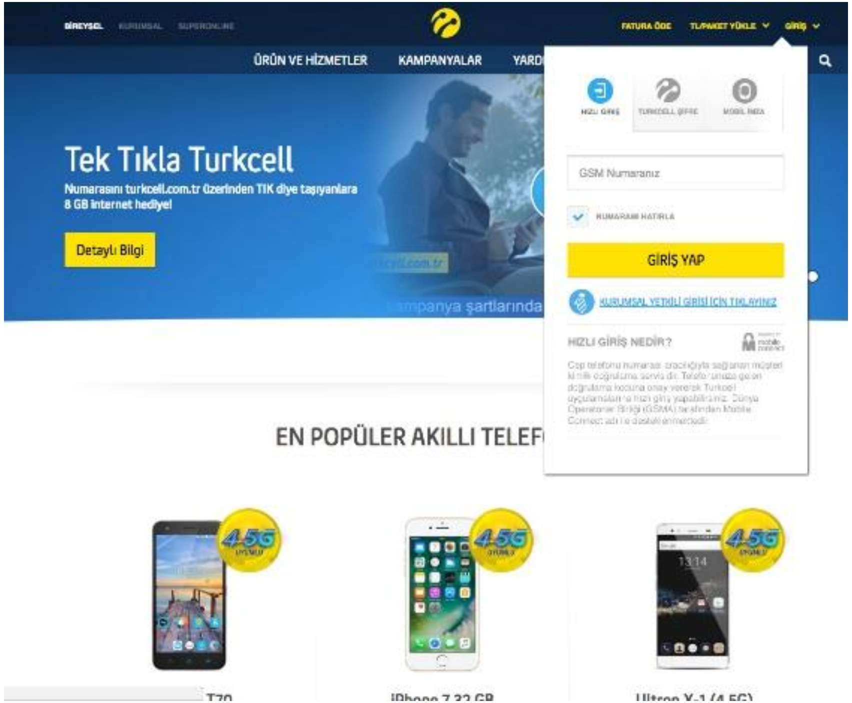
Solution A: For operators using a different service/product name



Scenario 1:
Where a compliant operator is using an existing service name for its mobile identity service and wishes to overtly reference Mobile Connect.

Scenario 2:
Where an operator is offering Mobile Connect and at the same time wants to flag a bespoke product as being accessed using Mobile Connect.

Scenario 1: Where an operator is offering a Mobile Connect and at the same time wants to a bespoke product or service uses Mobile Connect



BİREYSEL KURUMSAL SUPERONLINE

FATURA ÖDE TL/PAKET YÜKLE GİRİŞ

ÜRÜN VE HİZMETLER KAMPANYALAR YARD

Tek Tıkla Turkcell

Numarasını turkcell.com.tr üzerinden TIK diye taşıyanlara 8 GB internet hediye!

Detaylı Bilgi

kampanya şartlarında

HIZLI GİRİŞ TURKCELL ŞİFRE MOBİL İMZA

GSM Numaranız

☑ NUMARAMI HATIRLA

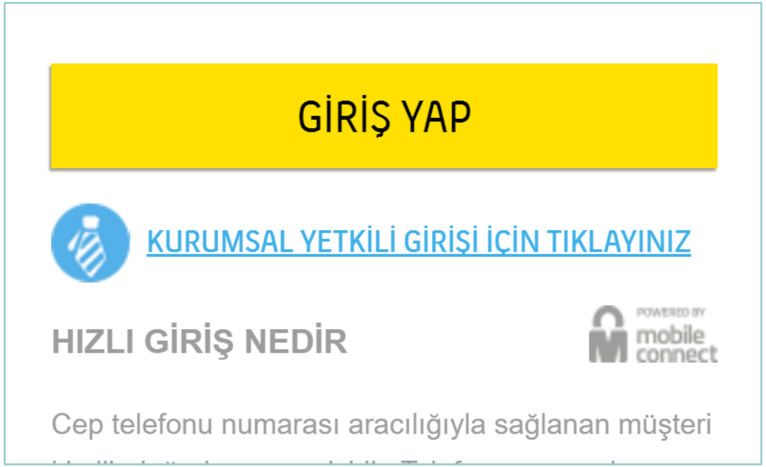
GİRİŞ YAP

KURUMSAL YETKİLİ GİRİŞİ İÇİN TIKLAYINIZ

HIZLI GİRİŞ NEDİR?

Cep telefonu numarası aracılığıyla sağlanan müşteri kimlik doğrulama servisidir. Telefonunuza gelen doğrulama kodunu onay vererek Turkcell uygulamalarına hızlı giriş yapabilirsiniz. Dünya Operatörler Birliği (GSMA) tarafından Mobile Connect adı ile desteklenmektedir.

EN POPÜLER AKILLI TELEF



GİRİŞ YAP

KURUMSAL YETKİLİ GİRİŞİ İÇİN TIKLAYINIZ

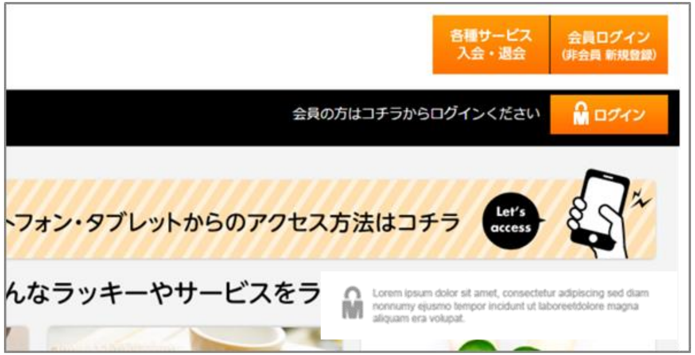
HIZLI GİRİŞ NEDİR

POWERED BY mobile connect

Cep telefonu numarası aracılığıyla sağlanan müşteri

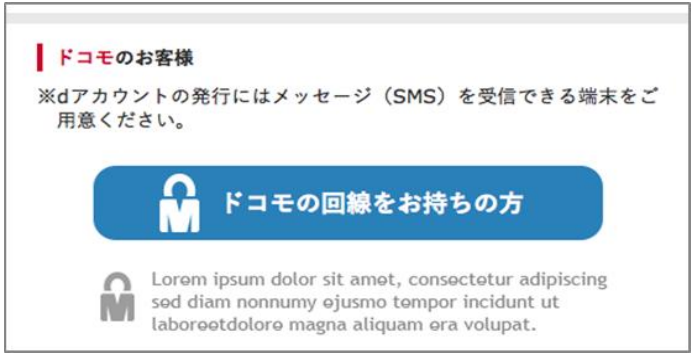
Solution B: For operators using a different service/product name

Scenario 3: Where operator has an existing service and service name that will “bridge” with Mobile Connect but does not yet wish to use the Mobile Connect name…



会員の方はコチラからログインください

Lorem ipsum dolor sit amet, consectetur adipiscing sed diam nonnumy ejusmo tempor incidunt ut laboreetdolore magna aliquam era volupat.



ドコモのお客様

※dアカウントの発行にはメッセージ（SMS）を受信できる端末をご用意ください。

Lorem ipsum dolor sit amet, consectetur adipiscing sed diam nonnumy ejusmo tempor incidunt ut laboreetdolore magna aliquam era volupat.

Example designs for illustrative purposes

Mobile Connect button used alongside existing service name, with explanation appearing close by

Current approach

Each case will continue to be evaluated on an individual basis.

Operators will be encouraged to use the Mobile Connect service mark, within the scenarios devised, where it provides a satisfactory solution for all parties.

However, there will undoubtedly be exceptions. These will be reviewed and a suitable compliant solution devised as required.

Planning stage: User flows & User experience consistency

Mobile Connect deployment guidelines for operators

Planning: User flows & UX consistency

- Operators to agree on flows, user screens (waiting screen, error screen etc.) and lifecycle events. It is recommended to use optimised user flows as excellent user experience is essential.

- Operators to obtain internal legal privacy sign off on user screen flows and ensure their alignment with the Mobile Connect privacy principles.

- Operators to review end user flows for each operator to ensure consistency and alignment taking into account any authenticator differences. Take into account the performance of the networks - e.g. page's size will have a UI impact.

- Although all operators should have a good UX, the UX does not have to be exactly the same across all MNOs.

Key learnings & best practices for UI deployments

User Education

- Brief introduction about Mobile Connect benefits for first time user.
- UI with concise messaging and a progress bar to guide the users during the process to avoid drop outs.
- Scale up user base by preregistering and providing incentives to activate the users.

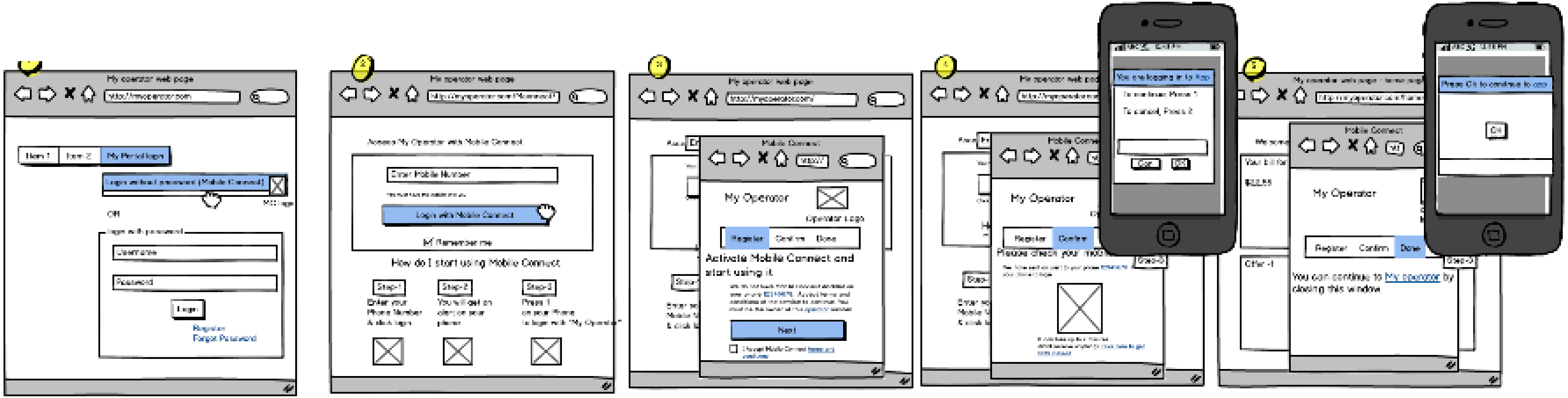
Building trust

- Instil trust in the service by exposing the user to familiar brands of the SPs and/or the operator.
- Clear and need to know basis textual/links removes potential confusion.
- Remove possibilities to deflect the user away from the UI and reduce drop out rates.

Deployment

- Thorough end-to-end testing is key to a successful role out of Mobile Connect.
- Pilot with internal operator-services in a controlled environment before scaling up.
- Optimise the user flows where possible with header enrichment and be aware of different flows depending on choice of authenticators.

Flow design: Key design principles summary



My operator web page
My Portal login
Login without password (Mobile Connect)
OR
Username
Password
Login
Register
Forgot Password
Access My Operator with Mobile Connect
Enter Mobile Number
Login with Mobile Connect
Remember me
How do I start using Mobile Connect
Step-1
Step-2
Step-3
Mobile Connect
My Operator
Operator Logo
Register
Confirm
Done
Activate Mobile Connect and start using it
Next
Please check your mobile
You are logging in to App
To continue, Press 1
To cancel, Press 2
Press Ok to continue to app
OK
You can continue to My operator by closing this window

Operator webpage | Mobile Connect login | Registeration screen | Waiting screen | Completion screen

Introducing Mobile Connect to new users:

- Introduce onto Operator Online Portals first and **set up analytics** to test the process and **identify any high dropout areas**
- **Keep the password option** so users have a choice of how to log-in
- Highlight & market the **key relevant message** for your local audience eg. "**log-in without a password using Mobile Connect**." This draws attention to the key differentiating factor and encourages users to try the new technology out.

Fast-track the Mobile Connect user registration process to convert users quickly:

- **Use Overlays** and **DO NOT** redirect to separate webpages or separate tabs. The **visibility of Operator branding is key** to maintain:
  - the **continuity** of the transaction between the operator & end user.
  - the **trust of the user** with the underlying operators brand and by association Mobile Connect
- Use a 3 or 4 step **progress bar** so the user knows what to expect next and when the process will finish
- Confirm that the user has successfully authenticated with Mobile Connect for the first time.

Design Look & Feel: Consistency across operators

Phase1: Planning

- Kick-off session with in-country Operators
- Identify Internal Services that have best fit for Mobile Connect
- Read the high level documentation
  - Operator Readiness Checklist
  - Test Suite Portal
  - Analytics Guide
- Select authenticators and enable Header Enrichment

Phase 2: Preparing

- Review end user flows for each operator to ensure consistency and alignment taking into account any authenticator differences.
- Familiarise and align on user guide, wire-frames, designs & HTML/CSS code.
- Agree on approach to minimise any UX/UI differences across country operators.
- Select consistent colour and branding logos
- Agree on messaging for introducing Mobile Connect

Phase 3: Beta Launch

- Launch close-beta
- Monitor performance and review analytics across Operators.
- Focus on jointly solving cross operator issues
- Collaborate on subscriber registration, marketing campaigns and ways to auto-enrol users for Mobile Connect accounts.
- Launch marketing initiatives to convert Mobile Connect Users Mobile Connect User Advocates for successful SP engagements

Planning stage: Local regulatory analysis

Mobile Connect deployment guidelines for operators

Planning: Regulatory requirements

- Operators should carry out local regulatory requirements analysis before deploying Mobile Connect.
- Special attention should be paid to local personal data protection and data transfer laws.
- It is important to understand if personal data can be transferred outside of your country.
- Early engagement with governments has multiple benefits for operators digital identity business enabling the generation of incremental revenues with positive impact on the digital economy:
  - Governments adoption of Mobile Connect can drive incremental revenues for operators by promoting the primary use of Mobile Connect across all sectors of the economy and leveraging the consumers perception of government reputation and establishment.

mobile connect

GSMA Identity

Planning stage: Mobile Connect Privacy Principles compliance

Mobile Connect deployment guidelines for operators

Planning: Mobile Connect privacy principles compliance

- The Mobile Connect Privacy Principles are intended to guide the use of personal information in the provision of Mobile Connect identity services by operators to third party service providers.

- The principles are ‘user centred’ and based on a common understanding that individuals have the right to expect that those who design, implement and operate identity services are committed to ensuring good privacy and security practices that respect and protect the privacy of individuals and the security of their data.

- Operators deploying Mobile Connect must comply with these privacy principles.

Planning stage: Project resources/governance

Mobile Connect deployment guidelines for operators

Planning: Project resources/governance

- Operators should identify dedicated project leads and allocate commercial, product, SP, marketing, legal, technical resources.
- There should be an established project governance model (e.g. Steering Committee and workstreams).
- Business owners should have full ownership and be able to drive Mobile Connect implementation process: the GSMA can only provide support and guidance.

Planning: Project resources/governance

There should be an established project governance model (e.g. Steering Committee and workstreams).

Operators should identify dedicated project leads and allocate commercial, product, SP, marketing, legal, technical resources.

Business owners should have full ownership and be able to drive Mobile Connect implementation process: the GSMA can only provide support and guidance.

Technical implementation stage: Implementation

Mobile Connect deployment guidelines for operators

Technical implementation: Implementation

- This is a technical implementation stage, where operators deploy Mobile Connect OIDC & Identity Gateway & API Exchange.

- They also must integrate authenticators and put relevant analytics in place for all of the deployed components. Analytics should capture traffic numbers, performance KPIs etc.

mobile connect

GSMA Identity

Technical implementation stage: Testing

Mobile Connect deployment guidelines for operators

Testing

API compatibility testing

Test Mobile Connect interoperability at the Mobile Connect Interoperability portal provided by GSMA.

Performance testing

Conduct performance testing (load, stress, capacity) for your ID Gateway. GSMA can provide testing scenario guidelines.

End-to-end testing

Carry out end-to-end tests with provisioned applications/services.

UX testing

Test the user flows and identify any high user dropout areas. Monitor performance and review/optimise user flows.

API compatibility testing- https://testsuite.mobileconnect.io/

What is it?

The site provides a suite of tests that check the Mobile Connect interface or platform meets the GSMA Mobile Connect specifications. The focus of the test suite is to validate the Mobile Connect API compatibility for **interoperability** and ensure a problem-free experience for end users.

Why Interoperability?

- Interoperability is a key proposition requirement of Mobile Connect and hence also one of the core requirements of the Mobile Connect licence agreement.
- It enables use of common tools, e.g. SDKs or the Mobile Connect Developer Portal.

Why Testing?

- Interoperability is a difficult beast and cannot be ensured without explicit and common testing.
- For Technology & Platform partner, operators get the assurance that they will not see “surprises” after deployment.
- Prevents from upsetting service providers by misusing them as our “test house”.

The Test Suite allows APIs for testing of the following Mobile Connect products : Authentication, (LoA 2 and 3), Authorisation (LoA2 and 3) and Identity products (including MC Phone Number, Sign-up and National ID).

Pre-launch stage: Service provider on-boarding

Mobile Connect deployment guidelines for operators

SP on-boarding: identify, qualify & approach SPs

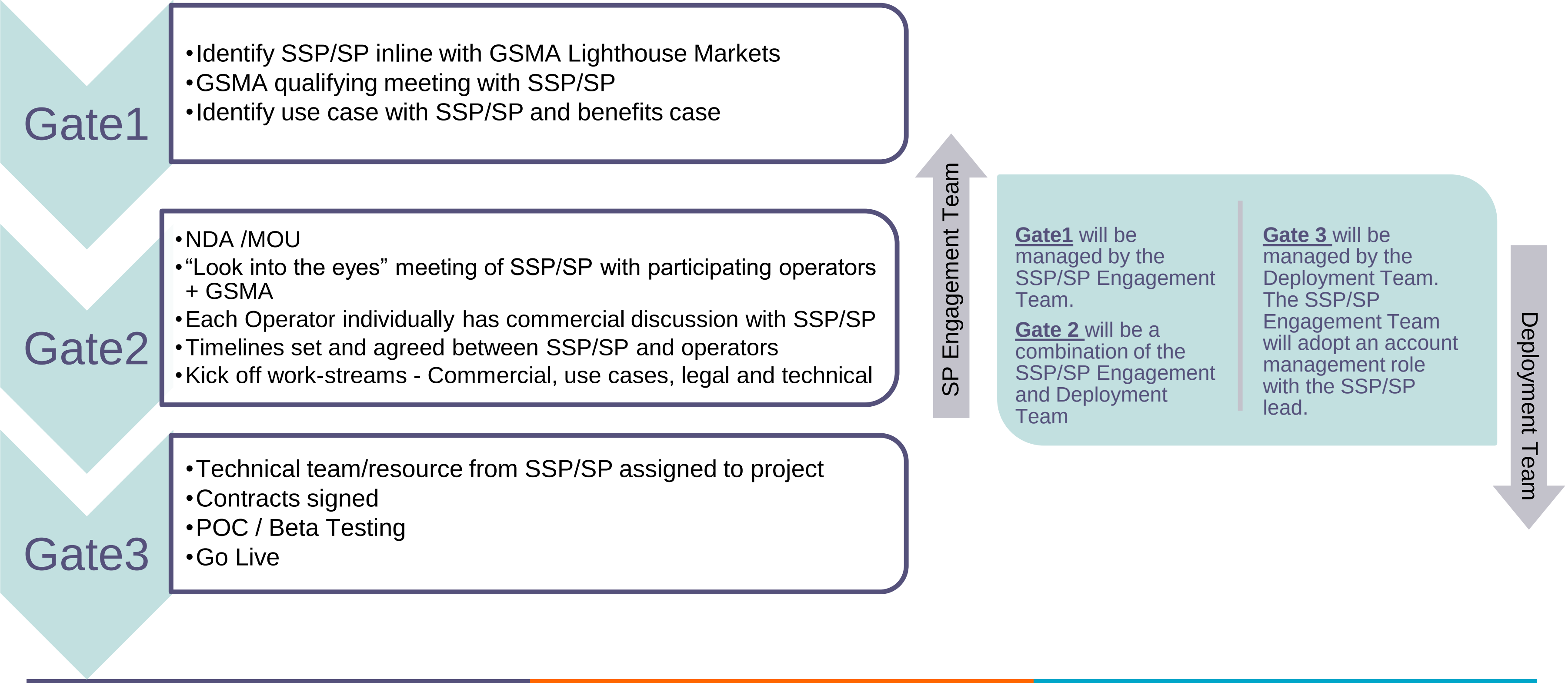
- **Identify** service provider candidates & potential use cases and approach target SPs.

- GSMA SP outreach team can support operators with the SP outreach. However, GSMA has a very limited SP outreach team that will focus only on the key SPs and business development opportunities. To facilitate this activity, the GSMA SP outreach team must have **access to the right business people** within the operator (e.g. P&L owners, enterprise sales leads).

- **Develop pricing model**. Even if you deploy only free services (e.g. basic authentication), it is essential to define a future path to monetisation.

- Have SP **billing & reconciliation capability in place**. Not relevant if you deploy only free services (e.g. basic authentication).

12 SP on-boarding steps



Gate1

- Identify SSP/SP inline with GSMA Lighthouse Markets
- GSMA qualifying meeting with SSP/SP
- Identify use case with SSP/SP and benefits case

Gate2

- NDA /MOU
- "Look into the eyes" meeting of SSP/SP with participating operators + GSMA
- Each Operator individually has commercial discussion with SSP/SP
- Timelines set and agreed between SSP/SP and operators
- Kick off work-streams - Commercial, use cases, legal and technical

Gate3

- Technical team/resource from SSP/SP assigned to project
- Contracts signed
- POC / Beta Testing
- Go Live

SP Engagement Team

Gate1 will be managed by the SSP/SP Engagement Team.

Gate 2 will be a combination of the SSP/SP Engagement and Deployment Team

Gate 3 will be managed by the Deployment Team. The SSP/SP Engagement Team will adopt an account management role with the SSP/SP lead.

Deployment Team

SP on-boarding: Commercial model

Operators should agree on a commercial model (e.g. direct contacting - every MNO contracts with every SP; wholesale - MNOs selling on behalf of each other).

Make available commercial contracts to SPs/SSPs and sign the contracts.

Allocate enough time for contracting as this process can be time-consuming.

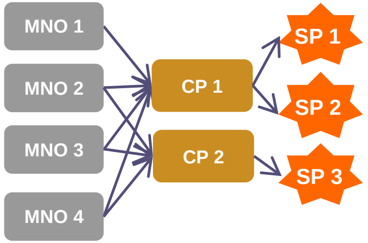
Commercial federation within country can be achieved through alternative structures to suit local preferences.

In-country commercial federation models – existing and planned

(in addition to direct sales each MNO to each SP)

Partner model

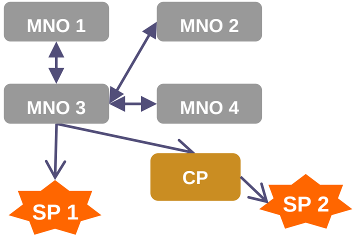
Operators sign agreements with partners to go to market on their behalf
Partner may also handle technical on-boarding



Estonia: partner is public certificate authority for tech & commercial on-boarding. 1,000+ SPs.
India: single technical platform; C2A + dev portal (free of charge); now looking for channel partners. ~15 SPs.
Pakistan: C2A + dev portal (free of charge); now looking for channel partners. ~10 SPs.
Bangladesh, Myanmar, Sri Lanka + others using C2A + dev portal.
~20 SPs per operator.

Lead MNO model

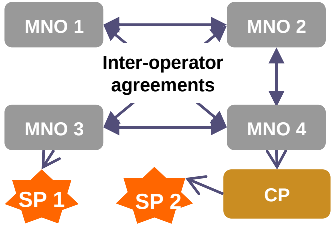
A lead operator signs agreements with other MNOs to go to market on their behalf



Switzerland: Swisscom is acting as lead operator for commercial and technical on-boarding. Inter-operator distribution of revenue (minus some direct costs).
100+ SPs.

Inter-operator model

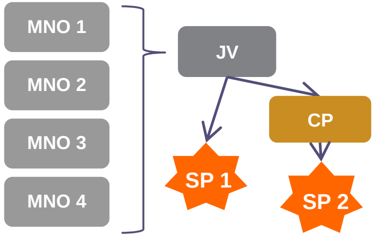
Operators sign agreements between each other and to go to market on each others behalf



Finland: Circle of Trust between operators. Competition between MNOs to sell to SPs. Tech and com on-boarding on behalf of other MNOs. Inter-operator settlement. 300+ SPs
Spain: working on inter-operator agreements where MNOs are able to take the lead for SPs and represent each other commercially. 1 SP.
UK: considering inter-operator agreements. 1 SP.

Operator JV model

Operators create a Joint Venture to go to market on their behalf



Norway: BankID is a JV between banks collaborating with MNOs. Common "BankID" branding. 100+ SPs
Canada: JV between operators is offering MC pilot. Each operator retains their branding. 3 SPs in pilot.
Taiwan: JV between MNOs to build and run a federated platform.
Netherlands: considering JV together with banks.

Pre-launch stage: End user and service provider support

Mobile Connect deployment guidelines for operators

Pre-launch: End user and SP support

Operators must establish customer support (end user to SP/MNO, SP to MNO) with a clearly defined support model, SLAs and processes.

Pre-launch Stage: Marketing, PR, consumer incentivisation

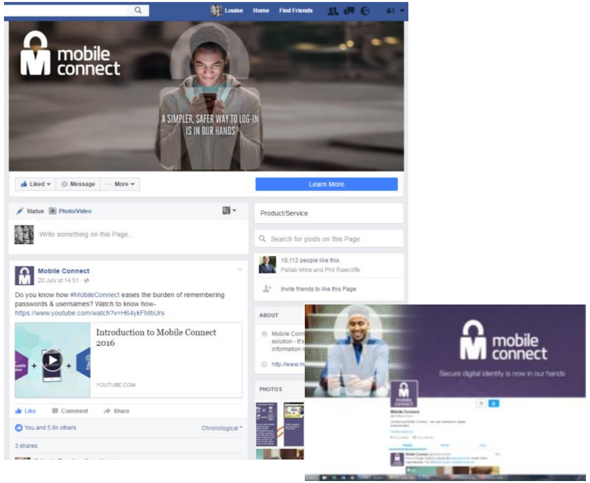
Mobile Connect deployment guidelines for operators

Marketing overview

Generating consumer awareness/user registration requires a **solid working product with a clear consumer CTA**(i.e. access points via launched digital services and operator products), as well as the **opportunity to experience Mobile Connect** on user services in a positive manner, demonstrating clear benefits to the consumer.

Operator need to create or point to Mobile Connect **consumer education materials**, ideally on their own websites, and social media platforms.

Marketing awareness/educational activity is **stronger when associated with well-known consumer brands**. It should target existing users familiar with and with an intrinsic trust of operator brands through their mobile contract. Therefore, joint marketing originated from operator in partnership with service provider brands will be the most effective way to educate consumers.


mobile connect
A SIMPLER, SAFER WAY TO LOG-IN IS IN OUR HANDS
Liked
Message
More
Learn More
Status
Photo/Video
Write something on this Page...
Product/Service
Search for posts on this Page
10,112 people like this
Invite friends to like this Page
ABOUT
PHOTOS
Like
Comment
Share
You and 5.8k others
Chronological
3 shares
Secure digital identity is now in our hands

Mobile Connect
20 July at 14:51
Do you know how #MobileConnect eases the burden of remembering passwords & usernames? Watch to know how- https://www.youtube.com/watch?v=H64yKFMbUrs
Introduction to Mobile Connect 2016
YOUTUBE.COM

Working together

GSMA can provide support

- **A consumer website**, in relevant languages, if required.
  - See www.mobileconnect.io / www.mobileconnect.in for example
- **Global Mobile Connect social media feed** with organic content feed pointing to live services. *(see examples below)*
  - **Twitter:** @mobileconnect
  - **Facebook:** @mobileconnectofficial
  - **U-Tube Playlist:** Identity at The GSMA
- **Campaign suggestions/best practice ideas** that can be personalised to fit operator service and provider brand messaging requirements
- **Content generation and messaging support** for campaign activities
- **Global content repository** including graphics, animated graphics, video and web assets for operators/SPs to use and/or personalise.
  - http://brand.mobileconnect.io/
- **Support for customer insight/research/focus group** activities to identify consumer pain points and user experience understandings.

Operator should provide

- **Dedicated marketing support** from their own marketing team and ensure agreement to support marketing activities
- **Marketing resource and budget** to manage/run campaign activity within own organisation and manage marketing plans.
- **Commitment to working together** with the other operators/SPs in country on a joint marketing activity plan.
- **Customer call to action** – i.e. services where the consumer can use Mobile Connect:
  - Operator own services
  - Service providers

Branded marketing activities

- Co-partnered/branded content on social media
- Operator use of Mobile Connect for own services
- Operator web page for Mobile Connect
- Targeted SMS campaigns
- Ambassador programmes
- Developer forums/chat rooms with App Challenge/hackathon activities
- Consumer incentive campaigns
- Target blogger/tech press for influencer activity.
- Consumer and business PR

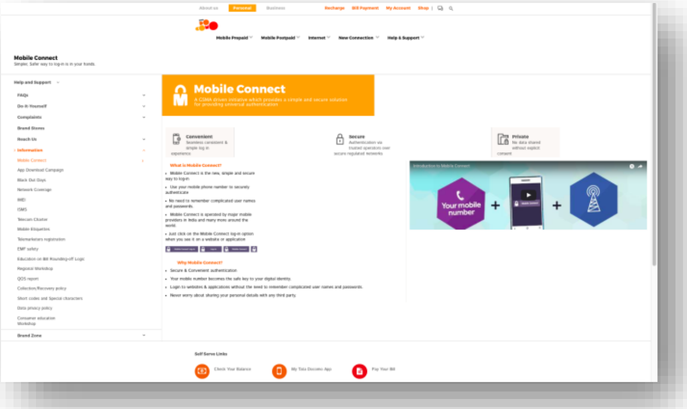
Forget Usernames and Passwords
Use Mobile Connect
A simpler, safer way to log-in
Register today
vodafone

mobile connect
Idea
Mobile Connect makes your mobile number your access-all password.
Never be locked out of your accounts again!

Pre-launch stage: Operator Mobile Connect marketing examples

Mobile Connect deployment guidelines for operators

India: Tata Docomo



About us | Personal | Business | Recharge | Bill Payment | My Account | Shop

Mobile Prepaid | Mobile Postpaid | Internet | New Connection | Help & Support

Mobile Connect

Simple; Safer way to log-in is in your hands.

Help and Support
- FAQs
- Do-It-Yourself
- Complaints
- Brand Stores
- Reach Us
- Information
  - Mobile Connect
  - App Download Campaign
  - Black Out Days
  - Network Coverage
  - IMEI
  - ISMS
  - Telecom Charter
  - Mobile Etiquettes
  - Telemarketers registration
  - EMF safety
  - Education on Bill Rounding-off Logic
  - Regional Workshop
  - QOS report
  - Collection/Recovery policy
  - Short codes and Special characters
  - Data privacy policy
  - Consumer education Workshop
- Brand Zone

Mobile Connect

A GSMA driven initiative which provides a simple and secure solution for providing universal authentication

Convenient Seamless consistent & simple log in experience

Secure Authentication via trusted operators over secure regulated networks

Private No data shared without explicit consent

What is Mobile Connect?
- Mobile Connect is the new, simple and secure way to log-in
- Use your mobile phone number to securely authenticate
- No need to remember complicated user names and passwords.
- Mobile Connect is operated by major mobile providers in India and many more around the world.
- Just click on the Mobile Connect log-in option when you see it on a website or application

Why Mobile Connect?
- Secure & Convenient authentication
- Your mobile number becomes the safe key to your digital identity.
- Login to websites & applications without the need to remember complicated user names and passwords.
- Never worry about sharing your personal details with any third party.

Introduction to Mobile Connect

Self Serve Links

Check Your Balance | My Tata Docomo App | Pay Your Bill

Shop. Pay bills. Simply. Securely. mobile connect

mRUPEE

SHOP. PAY BILLS. SECURELY. SIMPLY.

POWERED BY mobile connect

December:

- Promoting Mobile Connect YouTube video page on GET App Wall in order to increase awareness and drive education. (20th Dec – ongoing)
- New Year Special Promotion through GET App – Showcasing Mobile Connect Video to Users (1st Jan’17)
- New Year Special promotions of Mobile Connect on GET App Facebook page. (30th Dec-1st Jan).
- Promoting Mobile Connect on Tata Docomo Website. Your stats also shows traffic routing from Tata Docomo website to Mobile Connect India Website (Ongoing since 19th July)
- Linked to www.mobileconnect.in

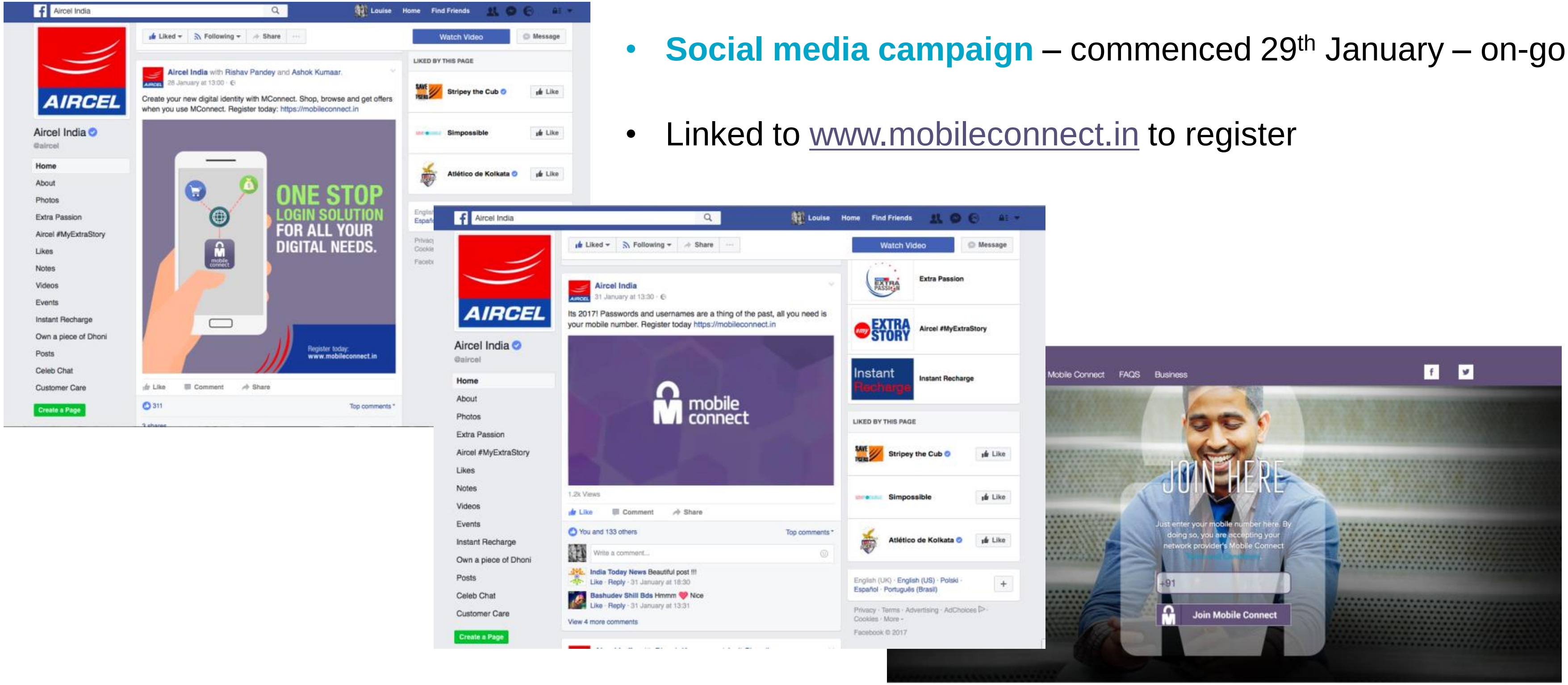
January:

- Continuing Promotion of Mobile Connect YouTube Video Page on GET App Wall in order to increase awareness and drive education.
- Banner placement in other portals.

India: Aircel

- **Social media campaign** – commenced 29th January – on-going

- Linked to www.mobileconnect.in to register



Aircel India with Rishav Pandey and Ashok Kumaar.
28 January at 13:00

Create your new digital identity with MConnect. Shop, browse and get offers when you use MConnect. Register today: https://mobileconnect.in

Aircel India
31 January at 13:30

Its 2017! Passwords and usernames are a thing of the past, all you need is your mobile number. Register today https://mobileconnect.in

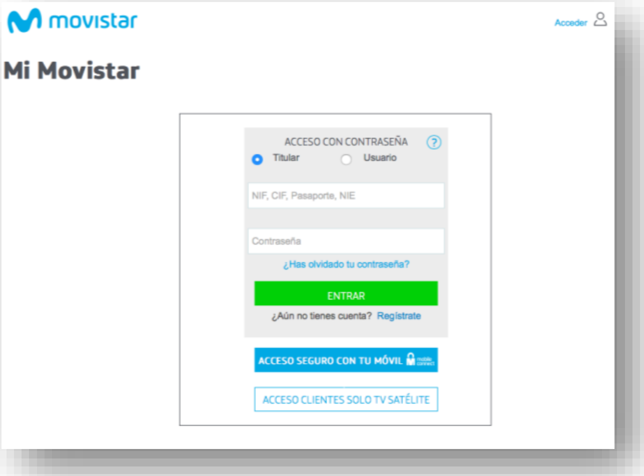
India Today News Beautiful post !!!

Bashudev Shill Bds Hmmm ❤ Nice

JOIN HERE

Just enter your mobile number here. By doing so, you are accepting your network provider's Mobile Connect

Spain: Telefonica – Mi Movistar



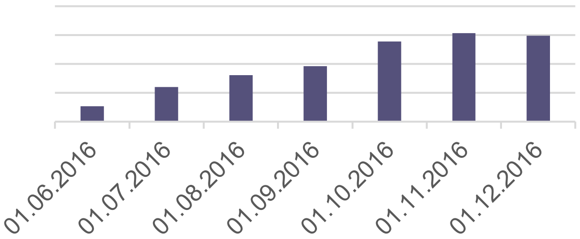
Telefonica Group deployed Mobile Connect in Spain at the end of 2015 on their self-care portal, Mi Movistar, with an objective to increase usage of this online channel. In order to drive take-up of the service, Telefonica Spain streamlined their registration flow and implemented a communications strategy.

- Simplify registration as much as possible – both the process itself and the content displayed
- Keep the underlying service brand (in this case the operator) visible during registration to increase user trust.
- Include Mobile Connect by default into new subscription contracts.
- Start marketing Mobile Connect to subscribers with a targeted 1-to-1 promotion towards selected users of the underlying service.
- Communicate Mobile Connect across channels as a “passwordless” method of accessing personal accounts
- Include this simple message in other promotional activity relating to the underlying service.

Results: Registrations to Mobile Connect have grown at over 50% per month during Q4 2016, while monthly transactions increased six fold between July and December 2016.

Spain: Telefonica – Summary of marketing activities

Monthly transaction volume on Mi Movistar



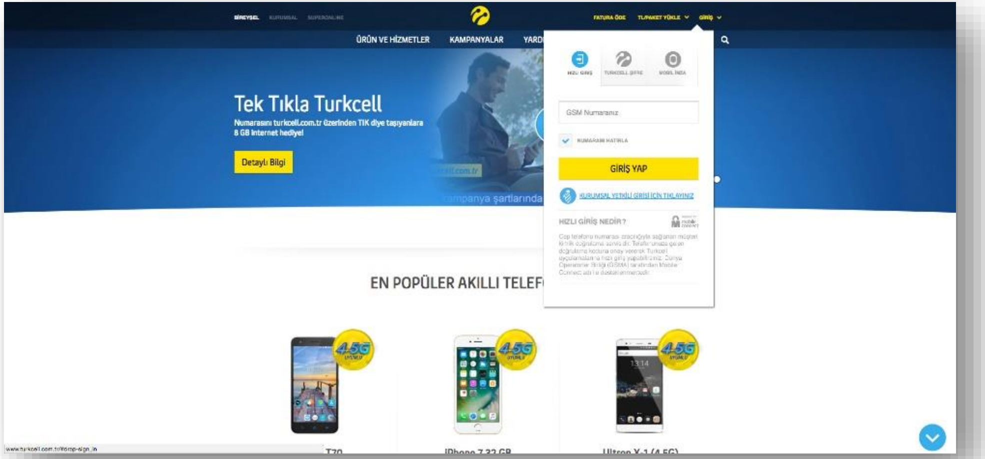
1. Targeted subscribers individually via email or phone to tell them about Mobile Connect in the hope that a simpler log-in option would encourage them to use the portal more often.
2. Amended contents of all the website "help" topics related to personal accounts to promote Mobile Connect as a passwordless method for users to access their private area.
3. The same message on banners in the help section, and presented to users who failed to enter their correct password when trying to access their account.
4. In parallel, encouraged usage of Mobile Connect on their various web properties and social media accounts, and call centres.
5. Created a video to explain the principle of Mobile Connect to end-users and an infographic to guide them through the journey and demonstrate its simplicity.

Results: The share of Mobile Connect in the total log-ins to Mi Movistar grew threefold in two weeks.

6. Encouraged users to switch to digital bills through an SMS campaign encouraging passwordless access to monthly bills online.
7. Additionally, a one-day push notification to users accessing the website induced a peak of activity – pushing traffic up to four time the usual daily transactions.
8. Gift card draws of a value of 500€ for customers accessing their online accounts or digital bills via Mobile Connect.

Results: The traffic in October grew by 44% compared to the previous month, before peaking in November

Turkey: Turkcell – Driving consumer usage



Consumer survey identified that the main reason users were not using the Mobile Connect login was simple lack of awareness of the product.

1. Changed the name of the login option to encourage uninformed people to try it
2. “Fast Login (powered by MC)” was chosen as the new branding and the interface was changed mid-December 2016.
3. Mobile Connect became the default login mechanism on their website and mobile app. This involved moving the “Mobile Connect login” tab from right-hand to left-hand, so it became the first option which users wanting to login would see.

Results:

80% increase in daily registrations.

In December 2016 14k subscribers were registering daily with a total of 40k Mobile Connect transactions daily

mobile connect

GSMA Identity

Launch stage

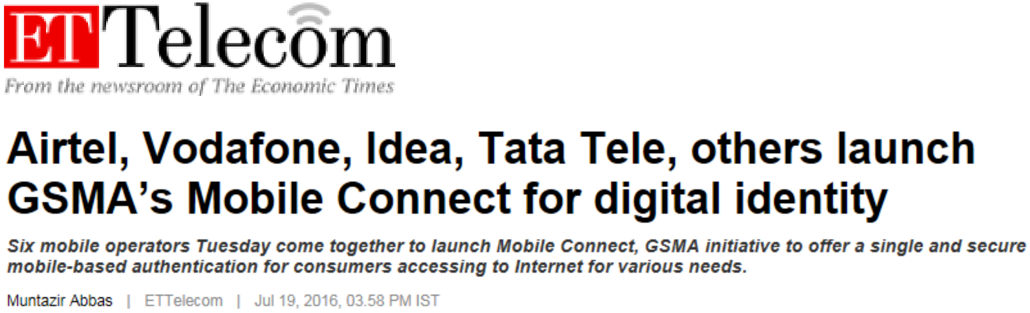
Mobile Connect deployment guidelines for operators

Launch: Public launch

Decide on public launch date and carry out pre-launch marketing campaign. Soft launch should be considered in advance of a full launch. Especially in markets which are not fully ready (technically/commercially/contractually) for the full launch.

It is recommended to launch Mobile Connect on your internal services first and/or conduct trials before the full public launch. Then at the public launch you will be able to share your customer success stories from trials and/or internal services.

India final launch coverage (5th August, 2016)



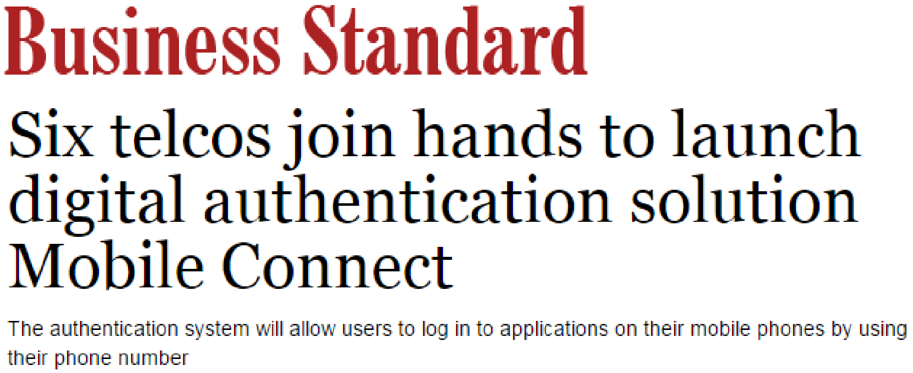
ETTelecom

From the newsroom of The Economic Times

Airtel, Vodafone, Idea, Tata Tele, others launch GSMA's Mobile Connect for digital identity

Six mobile operators Tuesday come together to launch Mobile Connect, GSMA initiative to offer a single and secure mobile-based authentication for consumers accessing to Internet for various needs.

Muntazir Abbas | ETTelecom | Jul 19, 2016, 03.58 PM IST



Business Standard

Six telcos join hands to launch digital authentication solution Mobile Connect

The authentication system will allow users to log in to applications on their mobile phones by using their phone number

28

attending media, including:
Business Standard
Business Today
CNBC TV18
DNA
Economic Times
Financial Express
IANS
PTI

50

Original coverage hits

29

Article syndications

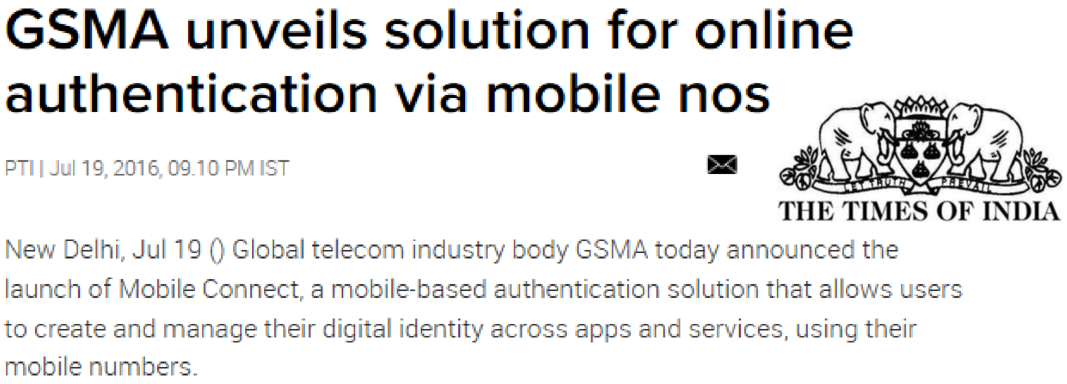
780

Press release syndications

859

Total coverage

India final launch coverage



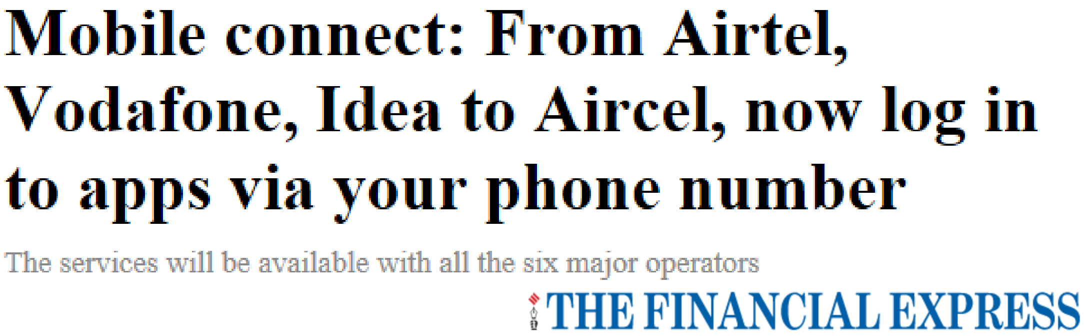
GSMA unveils solution for online authentication via mobile nos

PTI | Jul 19, 2016, 09.10 PM IST

THE TIMES OF INDIA

LET TRUTH PREVAIL

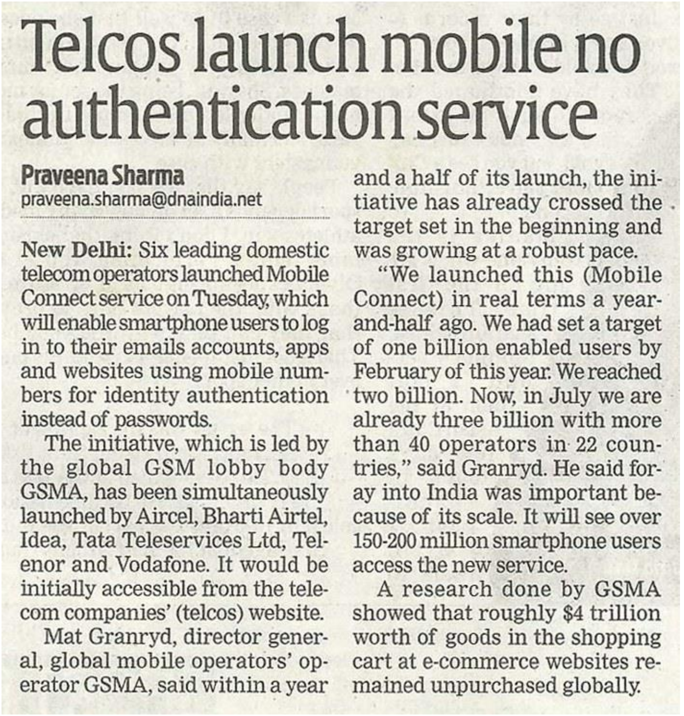
New Delhi, Jul 19 () Global telecom industry body GSMA today announced the launch of Mobile Connect, a mobile-based authentication solution that allows users to create and manage their digital identity across apps and services, using their mobile numbers.



Mobile connect: From Airtel, Vodafone, Idea to Aircel, now log in to apps via your phone number

The services will be available with all the six major operators

THE FINANCIAL EXPRESS



Telcos launch mobile no authentication service

Praveena Sharma
praveena.sharma@dnaindia.net

New Delhi: Six leading domestic telecom operators launched Mobile Connect service on Tuesday, which will enable smartphone users to log in to their emails accounts, apps and websites using mobile numbers for identity authentication instead of passwords.

The initiative, which is led by the global GSM lobby body GSMA, has been simultaneously launched by Aircel, Bharti Airtel, Idea, Tata Teleservices Ltd, Telenor and Vodafone. It would be initially accessible from the telecom companies' (telcos) website.

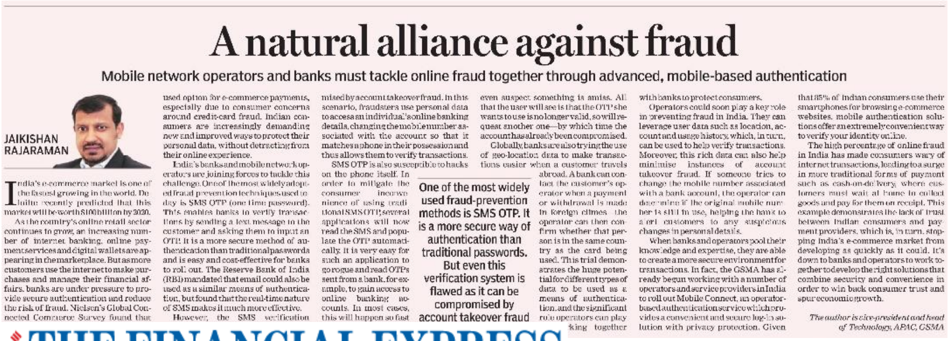
Mat Granryd, director general, global mobile operators' operator GSMA, said within a year and a half of its launch, the initiative has already crossed the target set in the beginning and was growing at a robust pace.

"We launched this (Mobile Connect) in real terms a year-and-half ago. We had set a target of one billion enabled users by February of this year. We reached two billion. Now, in July we are already three billion with more than 40 operators in 22 countries," said Granryd. He said foray into India was important because of its scale. It will see over 150-200 million smartphone users access the new service.

A research done by GSMA showed that roughly $4 trillion worth of goods in the shopping cart at e-commerce websites remained unpurchased globally.

India pre-launch by-line pitching

3 by-lines placed with key business media:



A natural alliance against fraud

Mobile network operators and banks must tackle online fraud together through advanced, mobile-based authentication

JAIKISHAN RAJARAMAN

India's e-commerce market is one of the fastest growing in the world. Deloitte recently predicted that this market will be worth $100 billion by 2020.

As the country's online retail sector continues to grow, an increasing number of internet banking, online payment services and digital wallets are appearing in the marketplace. But as more customers use the internet to make purchases and manage their financial affairs, banks are under pressure to provide secure authentication and reduce the risk of fraud. Nielsen's Global Connected Commerce Survey found that

used option for e-commerce payments, especially due to consumer concerns around credit-card fraud. Indian consumers are increasingly demanding new and improved ways to protect their personal data, without detracting from their online experience.

India's banks and mobile network operators are joining forces to tackle this challenge. One of the most widely adopted fraud prevention techniques used today is SMS OTP (one time password). This enables banks to verify transactions by sending a text message to the customer and asking them to input an OTP. It is a more secure method of authentication than traditional passwords and is easy and cost-effective for banks to roll out. The Reserve Bank of India (RBI) mandated that email could also be used as a similar means of authentication, but found that the real-time nature of SMS makes it much more effective.

However, the SMS verification mised by account takeover fraud. In this scenario, fraudsters use personal data to access an individual's online banking details, changing the mobile number associated with the account so that it matches a phone in their possession and thus allows them to verify transactions.

SMS OTP is also susceptible to hacks on the phone itself. In order to mitigate the consumer inconvenience of using traditional SMS OTP, several applications will now read the SMS and populate the OTP automatically. It is very easy for such an application to go rogue and read OTPs sent from a bank, for example, to gain access to online banking accounts. In most cases, this will happen so fast

One of the most widely used fraud-prevention methods is SMS OTP. It is a more secure way of authentication than traditional passwords. But even this verification system is flawed as it can be compromised by account takeover fraud

even suspect something is amiss. All that the user will see is that the OTP she wants to use is no longer valid, so will request another one—by which time the account has already been compromised.

Globally, banks are also trying the use of geo-location data to make transactions easier when a customer travels abroad. A bank can contact the customer's operator when a payment or withdrawal is made in foreign climes — the operator can then confirm whether that person is in the same country as the card being used. This trial demonstrates the huge potential for different types of data to be used as a means of authentication, and the significant role operators can play king together with banks to protect consumers.

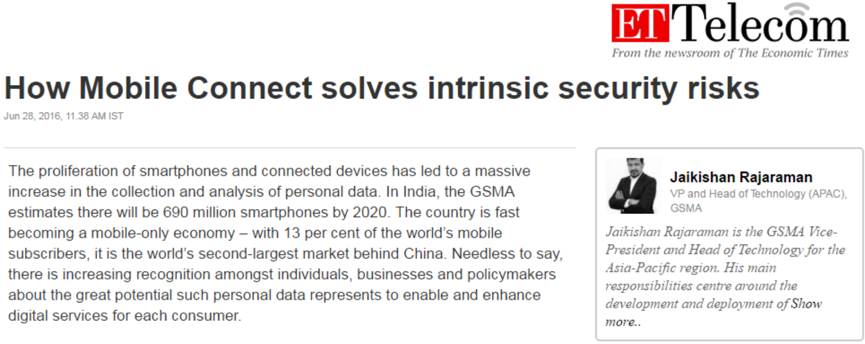
Operators could soon play a key role in preventing fraud in India. They can leverage user data such as location, account and usage history, which, in turn, can be used to help verify transactions. Moreover, this rich data can also help minimise instances of account takeover fraud. If someone tries to change the mobile number associated with a bank account, the operator can determine if the original mobile number is still in use, helping the bank to alert customers to any suspicious changes in personal details.

When banks and operators pool their knowledge and expertise, they are able to create a more secure environment for transactions. In fact, the GSMA has already begun working with a number of operators and service providers in India to roll out Mobile Connect, an operator-based authentication service which provides a convenient and secure log-in solution with privacy protection. Given that 85% of Indian consumers use their smartphones for browsing e-commerce websites, mobile authentication solutions offer an extremely convenient way to verify your identity online.

The high percentage of online fraud in India has made consumers wary of internet transactions, leading to a surge in more traditional forms of payment such as cash-on-delivery, where customers must wait at home to collect goods and pay for them on receipt. This example demonstrates the lack of trust between Indian consumers and payment providers, which is, in turn, stopping India's e-commerce market from developing as quickly as it could. It's down to banks and operators to work together to develop the right solutions that combine security and convenience in order to win back consumer trust and spur economic growth.

The author is vice-president and head of Technology, APAC, GSMA

THE FINANCIAL EXPRESS



ETTelecom
From the newsroom of The Economic Times

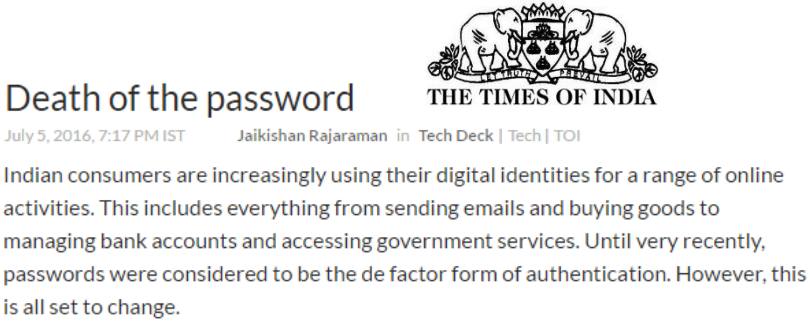
How Mobile Connect solves intrinsic security risks

Jun 28, 2016, 11.38 AM IST

The proliferation of smartphones and connected devices has led to a massive increase in the collection and analysis of personal data. In India, the GSMA estimates there will be 690 million smartphones by 2020. The country is fast becoming a mobile-only economy – with 13 per cent of the world's mobile subscribers, it is the world's second-largest market behind China. Needless to say, there is increasing recognition amongst individuals, businesses and policymakers about the great potential such personal data represents to enable and enhance digital services for each consumer.

Jaikishan Rajaraman
VP and Head of Technology (APAC), GSMA

Jaikishan Rajaraman is the GSMA Vice-President and Head of Technology for the Asia-Pacific region. His main responsibilities centre around the development and deployment of Show more..



THE TIMES OF INDIA

Death of the password

July 5, 2016, 7:17 PM IST   Jaikishan Rajaraman in Tech Deck | Tech | TOI

Indian consumers are increasingly using their digital identities for a range of online activities. This includes everything from sending emails and buying goods to managing bank accounts and accessing government services. Until very recently, passwords were considered to be the de factor form of authentication. However, this is all set to change.

mobile connect

India pre-launch interview pitching

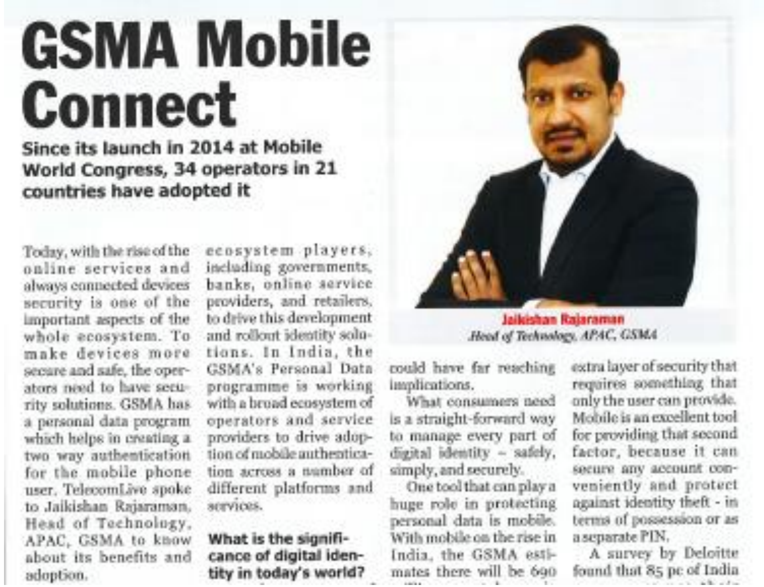
8 interviews with GSMA spokespeople conducted, including:

- Business Today
- Digit
- Fonearena
- Mint
- Telecom Lead
- Telecom Live
- Times of India

bt businesstoday.in

India roll out of Mobile Connect programme to happen soon: GSMA VP Marie Austenaa

TELECOM LIVE



GSMA Mobile Connect

Since its launch in 2014 at Mobile World Congress, 34 operators in 21 countries have adopted it

Jaikishan Rajaraman
Head of Technology, APAC, GSMA

Today, with the rise of the online services and always connected devices security is one of the important aspects of the whole ecosystem. To make devices more secure and safe, the operators need to have security solutions. GSMA has a personal data program which helps in creating a two way authentication for the mobile phone user. TelecomLive spoke to Jaikishan Rajaraman, Head of Technology, APAC, GSMA to know about its benefits and adoption.

ecosystem players, including governments, banks, online service providers, and retailers, to drive this development and rollout identity solutions. In India, the GSMA's Personal Data programme is working with a broad ecosystem of operators and service providers to drive adoption of mobile authentication across a number of different platforms and services.

What is the significance of digital identity in today's world?

could have far reaching implications.

What consumers need is a straight-forward way to manage every part of digital identity – safely, simply, and securely.

One tool that can play a huge role in protecting personal data is mobile. With mobile on the rise in India, the GSMA estimates there will be 690

extra layer of security that requires something that only the user can provide. Mobile is an excellent tool for providing that second factor, because it can secure any account conveniently and protect against identity theft - in terms of possession or as a separate PIN.

A survey by Deloitte found that 85 pc of India

India pre-launch marketing

During launch week

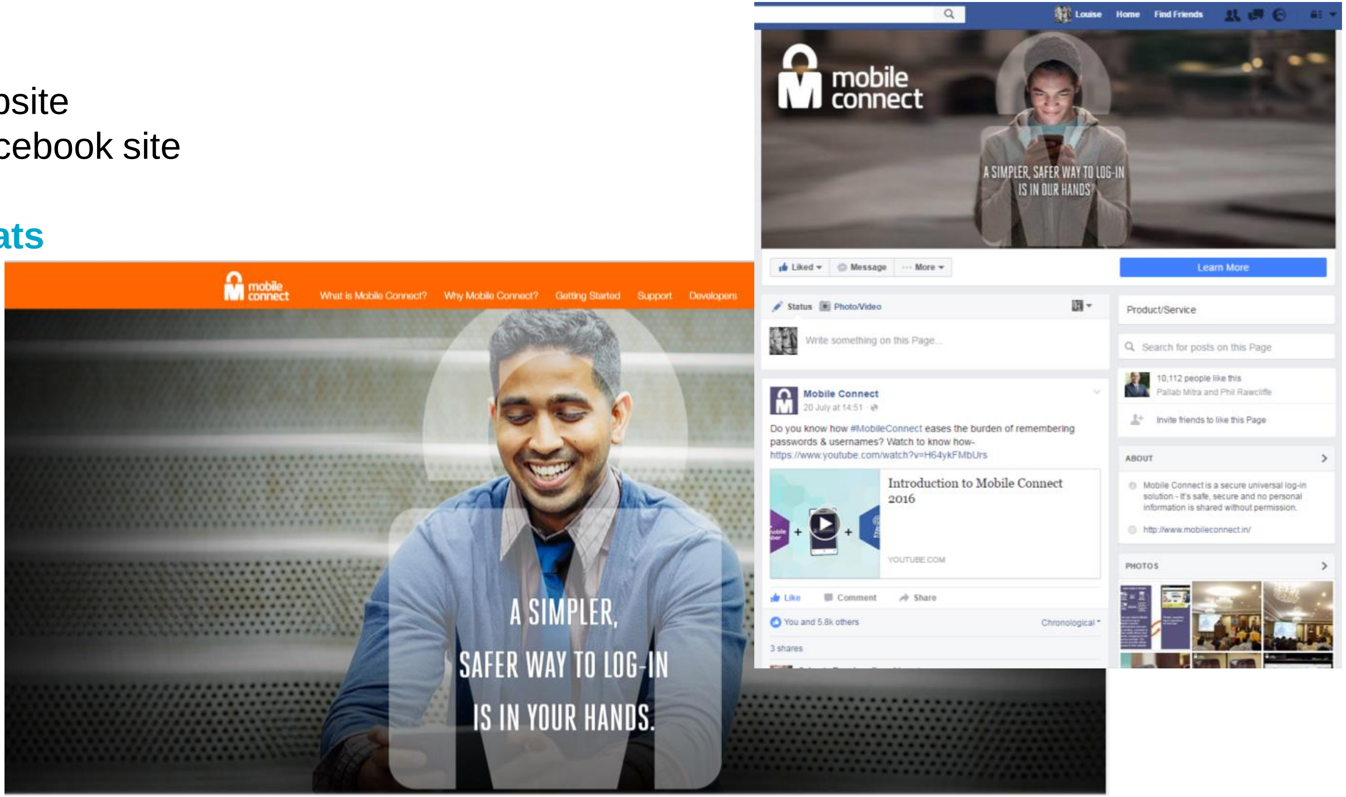
- 375,000 hits to the website
- 10,000 likes on the Facebook site

Current average daily stats

- 25k users/day
- 48k page views/day

Totals 9July to 8Aug

- 890,731 hits



Mobile Connect
20 July at 14:51

Do you know how #MobileConnect eases the burden of remembering passwords & usernames? Watch to know how-
https://www.youtube.com/watch?v=H64ykFMbUrs

Introduction to Mobile Connect 2016
YOUTUBE.COM

You and 5.8k others

3 shares

10,112 people like this
Pallab Mitra and Phil Rawcliffe

Mobile Connect is a secure universal log-in solution - It's safe, secure and no personal information is shared without permission.

http://www.mobileconnect.in/

Operational/BAU: Analytics and reporting

Mobile Connect deployment guidelines for operators

Operational/BAU: Analytics and reporting

- On-going service/user experience optimisation based on analytics.
- Operators internal and external (e.g. reporting Mobile Connect take-up and usage to GSMA) reporting requirements should be defined.

Appendix: Mobile Connect deployments

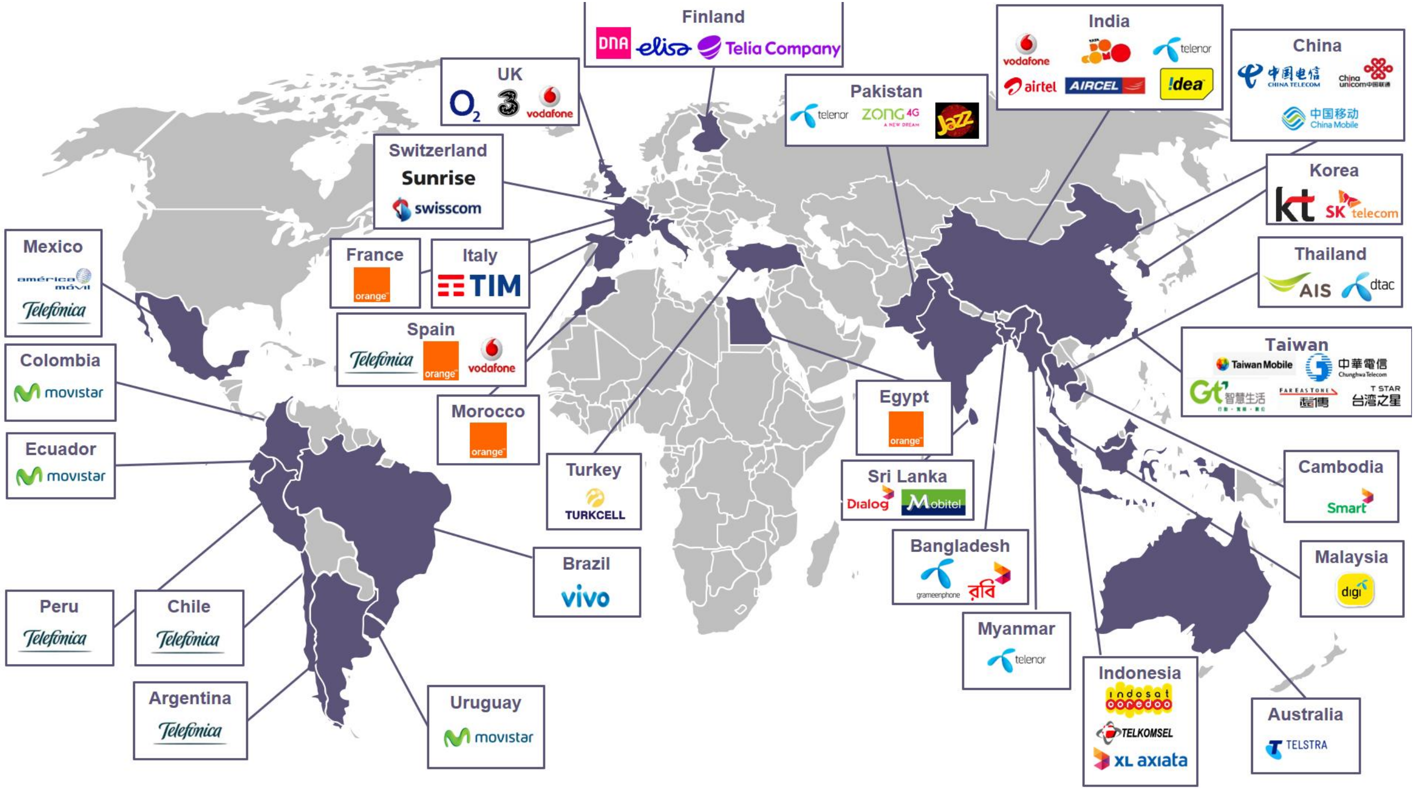
57 operators launched in 30 markets

3bn

Enabled users world-wide

105m

Mobile Connect registered users



If you would like more information, please contact the GSMA via:

mobileconnect@gsma.com

+44 (0) 20 7356 0600

www.gsma.com/identity
Follow the GSMA on Twitter: @GSMA

GSMA London Office
The Walbrook Building, 25 Walbrook, London EC4N 8AF