



Mobile Connect in Austria

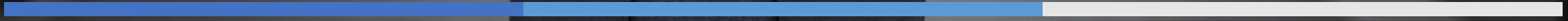
Operator round table meeting
hosted by RTR

08.10.2018, Vienna

- | | |
|----------------------|--|
| 9.00 – 9.10 | Welcome and introduction |
| 9.10 – 9:30 | Introductory remarks – RTR |
| 9.30 – 10.00 | Introduction to Mobile Connect – GSMA |
| 10.00 – 10.40 | Mobile Connect in Austria: What would it take? – GSMA |
| 10.40 – 11.00 | Coffee break |
| 11.00 – 11.30 | Mobile Connect in government applications - GSMA |
| 11.30 – 12:00 | Possibilities for participation of MVNOs - GSMA |
| 12.00 – 12.20 | Discussion – RTR |
| 12:20 – 12.30 | Closing remarks |



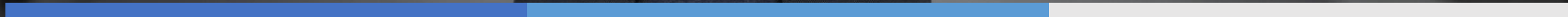
Welcome & introductions



GSMA antitrust notice – Mobile Connect

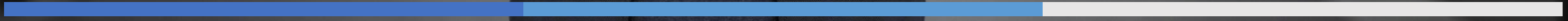
- Anti-trust law prohibits all agreements (written, verbal, or implicit) between competitors which may negatively impact the market or consumers
- Mobile Connect is an authentication, identity and attributes service offered to Service Providers, who are professional corporate buyers in a competitive market of solutions
- To be a feasible solution in the market Mobile Connect requires both technical and commercial level cooperation between mobile operators
- GSMA antitrust assessment has concluded that this cooperation is pro-competitive, on balance, and therefore likely to be permissible under applicable competition law
- Competition law regimes and market conditions differ between countries and regions. Operators are advised to seek local legal advice
- This presentation has been prepared in conjunction with GSMA antitrust policy

Introductory remarks
RTR





Introduction to Mobile Connect GSMA





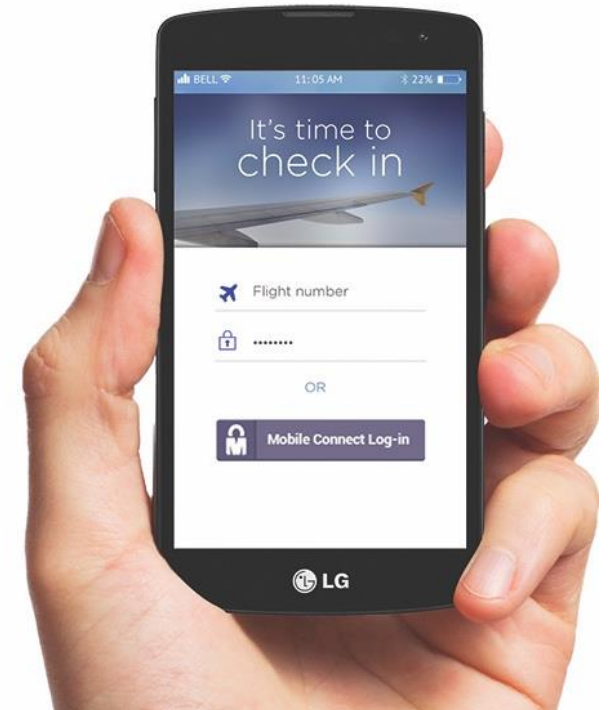
Mobile Connect is a mobile operator facilitated global digital identity solution

- **Mobile Connect** is a portfolio of mobile-based secure identity capabilities giving **simple, secure** and **convenient** access to online services
- Combines the user's unique mobile number and optional PIN to:
 - **Authenticate** users online
 - **Authorise** digital transactions and payments
 - Verify **identity**
 - Confirm **Attributes** about user or device
- Strong positive user feedback on usefulness and user experience resulting in significant take-up
- Positive position on privacy to ensure regulatory compliance and end-user trust as no personal information shared without consent
- 3bn enabled users; 473m active users
- 70 operators in 30+ markets

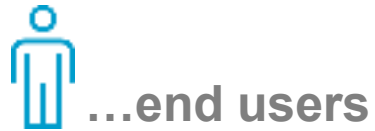


88% of consumers say a **single secure login solution would be beneficial**

Sources: GSMA Consumer Research 2015, Cyber Streetwise



Mobile Connect simplifies secure use of digital services



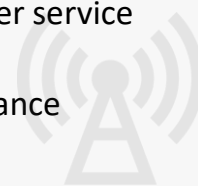
Simplifies & secures user's everyday life

- Convenience
- Remote Identity verification
- Improved security
- Builds trust
- Privacy control



Identity provides operators with a strategic position central to digital transformation

- Revenue opportunity from growing Identity market
- Strengthens operators' customer relevancy
- Enhanced value proposition to Enterprise
- Enhanced value proposition to service providers
- Extends reach to cross-border service providers
- Supports regulatory compliance



Enabling user identity: the foundation for businesses' digital innovation & transformation

- Increased conversion
- Improved security
- Global reach
- Reliable consent capture
- Fraud reduction
- Trusted device
- Regulatory compliance
- Customer Insight and Engagement
- Cost reduction & increased efficiency







Engaged global SPs



Use case examples

- Seamless and secure log-ins
- Convenient enhanced authentication
- Step-up authentication upon risk detection
- Convenient, secure payment authorisation
- Authorisation to add new payee to account
- Account sign-up
- Confirmation of user's identity
- Verify customer records to support know-your-customer (KYC) and anti-money laundering (AML) regulation
- Notice of fraud indicators (SIM change, active call diverts, device lost/stolen, account status)
- Verify user info and device for mobile wallet
- Verify validity of phone number change
- Age verification

Service roadmap

- Authentication**  Simple and globally ubiquitous log-in mechanism
- Authorisation**  Allow SPs to obtain authorisation from a user based on context
- Identity**  Provide user-identity data so SPs can fulfil digital services
- Attribute**  Protect personal data, prevent fraud and enable consent-based data exchange (network attributes)



Helping businesses identify their customers securely and conveniently

A combination of attribute verification and strong authentication



2005

SKT launch
T-Authentication

49%

of the Korean
market enabled

2017

Integrated into
Mobile Connect
framework

USE CASE 1: ATTRIBUTE VERIFICATION

- Leverages user account information held by the operator on their customers (name, address, ...)
- Check against information provided to service provider by the user
- Fulfills regulatory requirement for identity check when registering online

USE CASE 2: STRONG AUTHENTICATION

- 2-factor-authentication to securely log in to mobile apps (e.g. banking)
- Based on a SIM Applet + PIN combination
- Simple user experience (enter 6 digit PIN + submit)

As of early 2017

27,000 Korean
service providers are using
T-Authentication

13m monthly
active users

650m transactions
annually



IMPLEMENTING MOBILE CONNECT ON TURKCELL SERVICES TO DRIVE ADOPTION AUTHENTICATING CUSTOMERS FOR SELF-CARE MOBILE SITE



Dec 2015

Turkcell launch
Mobile Connect

33

Million enabled users

Live

on Turkcell online
portal & mobile app

BEFORE MOBILE CONNECT

- Need to remember a password
- If forgotten, can reset it via an SMS
- Mobile signature is the other option: hard to obtain, less than 0.1% of log-ins

AFTER MOBILE CONNECT

- Mobile number becomes their username
- Receive a Mobile Connect request on mobile and click "OK"
- No password to remember



Results

50% of all logins to Turkcell web portal now happen via Mobile Connect

97% of Mobile Connect users say they will use it again

1. Challenge and rationale

Payment services and other similarly regulated institutions encounter **challenges to verify customer details** during enrolment – which is a regulatory requirement.

This is key to **prevent identity theft** from occurring on their services.

2. Solution

Three has recently integrated with Danal to offer fraud prevention capabilities to service providers such as MoneyGram.

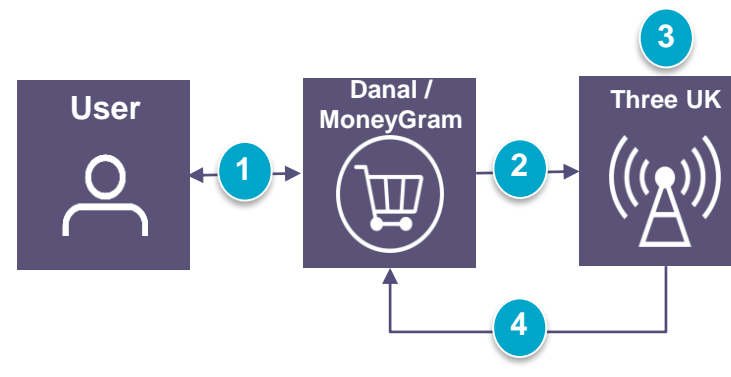
When a new customer registers onto MoneyGram, the name and address they enter are hashed and checked against the information which Three has on record for that mobile number.

MoneyGram gets a real-time confirmation of whether the registration information is genuine.

3. Benefits

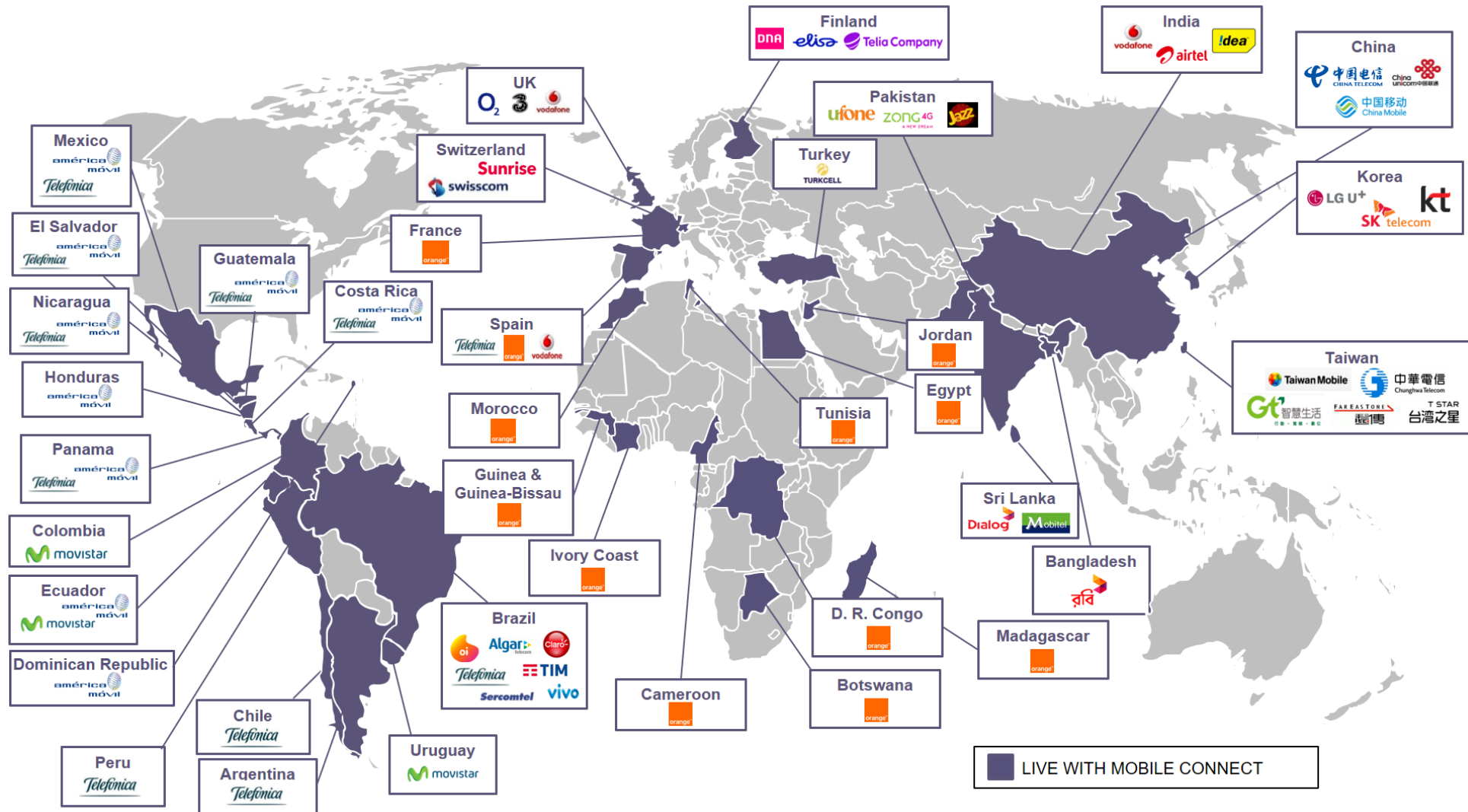
- ❑ Mobile operators offer dynamic, high quality data in real time
- ❑ Helps comply with Know-Your-Customer regulation
- ❑ Prevents occurrences of identity theft
- ❑ No disruption to customer journey
- ❑ Privacy protection – no new information is learnt by any party during the transaction

User flow



- 1 User registers to MoneyGram, who requests fraud check from Danal
- 2 Danal shares mobile number, hashed name and address with Three
- 3 Operator compares hashed information
- 4 Operator sends back indication of match

70 operators have deployed Mobile Connect in over 30 markets



Identity provides a major time-limited opportunity for operators to play a central role in ‘digital’ using Mobile Connect, a fundamental enabler and catalyst for the market.

Mobile Connect...

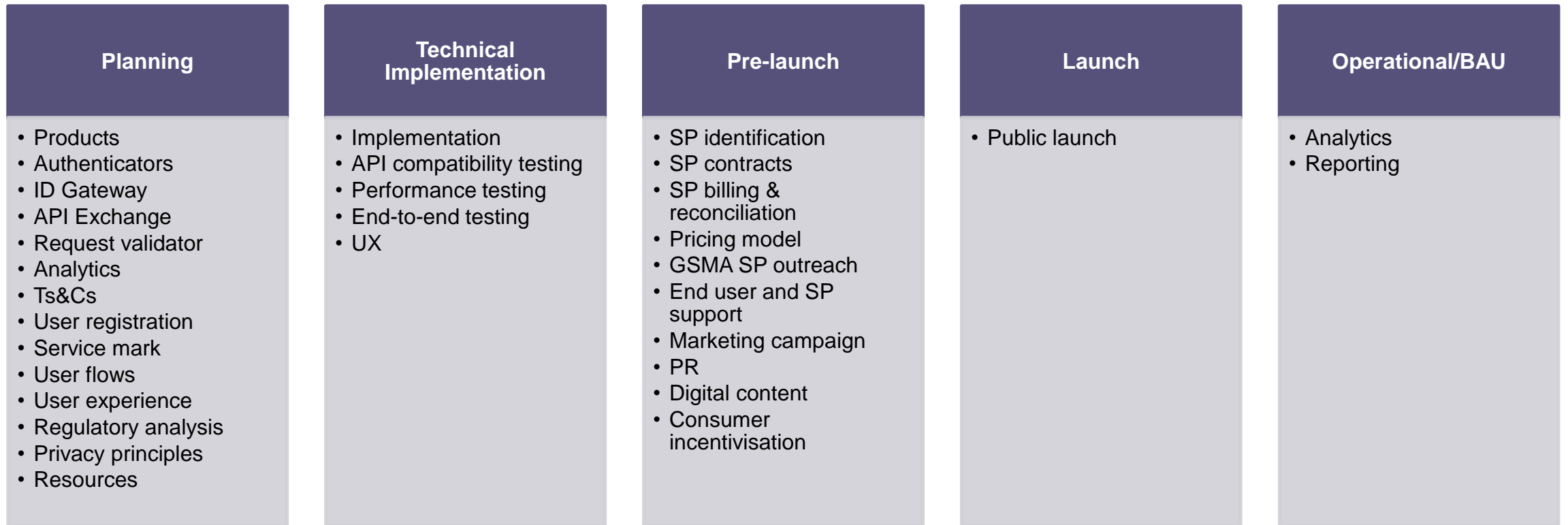
- ...is the only platform that globally aggregates the unique value operators can provide for identity whilst maintaining control of it
- ...provides operators with more strategic options than they have without it
- ...is building the rails for ecosystem reliance on operators’ assets

join us on the journey!

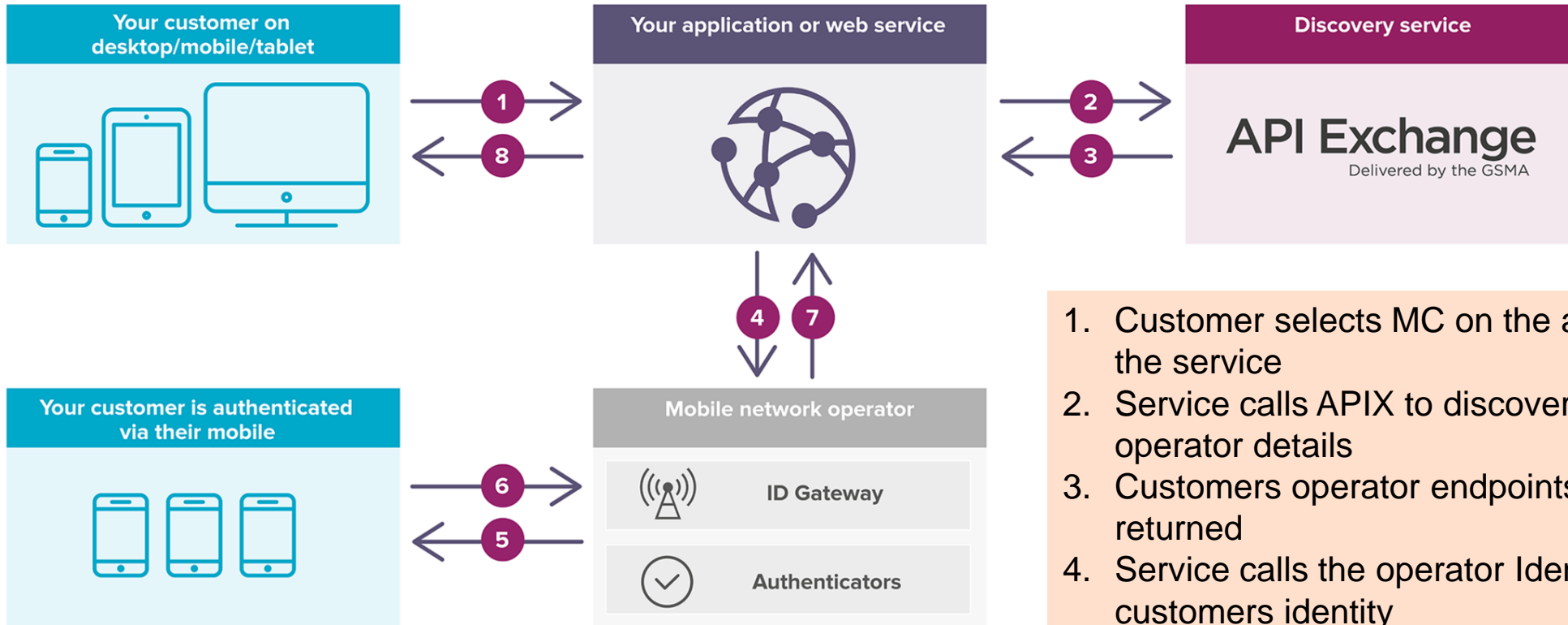


Mobile Connect in Austria
What would it take?

Deployment stages and activities

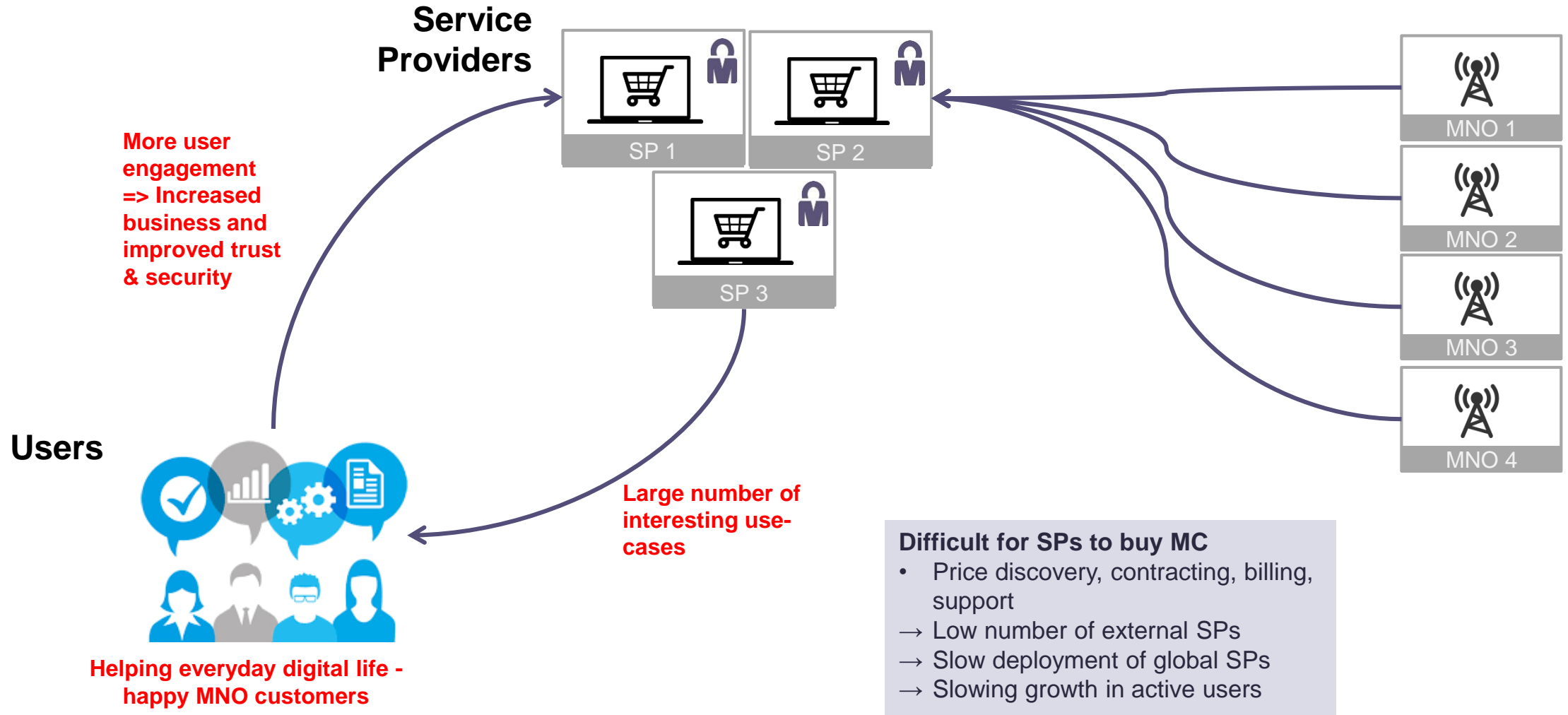


Mobile Connect – quick overview



1. Customer selects MC on the app / browser to access the service
2. Service calls APIX to discover customer's mobile operator details
3. Customer's operator endpoints and credentials returned
4. Service calls the operator Identity Service to verify customer's identity
5. Identity Service sends prompt to customer's mobile
6. Customer authenticates via the mobile
7. Identity Service returns confirmation to service
8. Service open to customer

To drive active users, MC must be used in many places - but difficulties to buy are preventing growth in services using MC



Customers (Service Providers) expect a joint single service

- Consistent Mobile Connect functionality across all mobile users
- Robust, scalable and commercially ready service
- Simple technical integration to reach all mobile users
- Simple sales and account manager
- Simple contract (including clear allocation of liabilities)
- Single set of prices
- Single bill and settlement process
- Single support function (both during on-boarding and in-life)
- Service monitoring

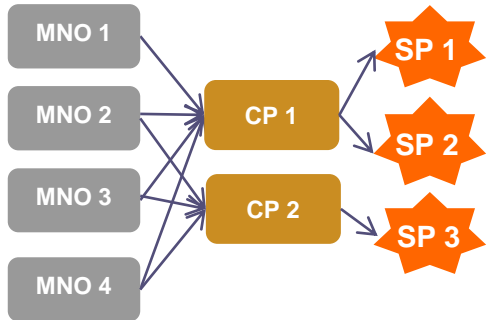
We need a simple business structure for Mobile Connect in the market

=> Commercial federation

Existing in-country commercial federation models

Partner model

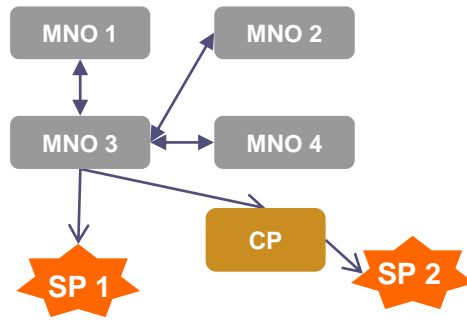
Operators sign agreements with partners to go to market on their behalf
Partner may also handle technical on-boarding



Relevant when time to market is critical

Lead MNO model

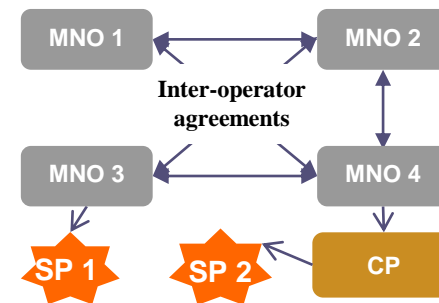
A lead operator signs agreements with other MNOs to go to market on their behalf



Relevant in fewer markets

Inter-operator model

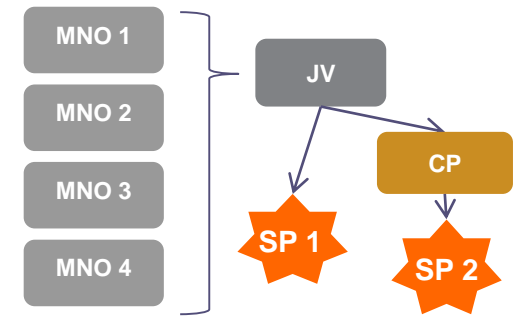
Operators sign agreements between each other to go to market on each other's behalf



Relevant when operators want to sell enablement services

Operator JV model

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



Relevant in fewer markets

Estonia: partner is public certificate authority for tech & commercial on-boarding. 1,000+ SPs.

Korea: 9 agents; 30,000 SPs

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

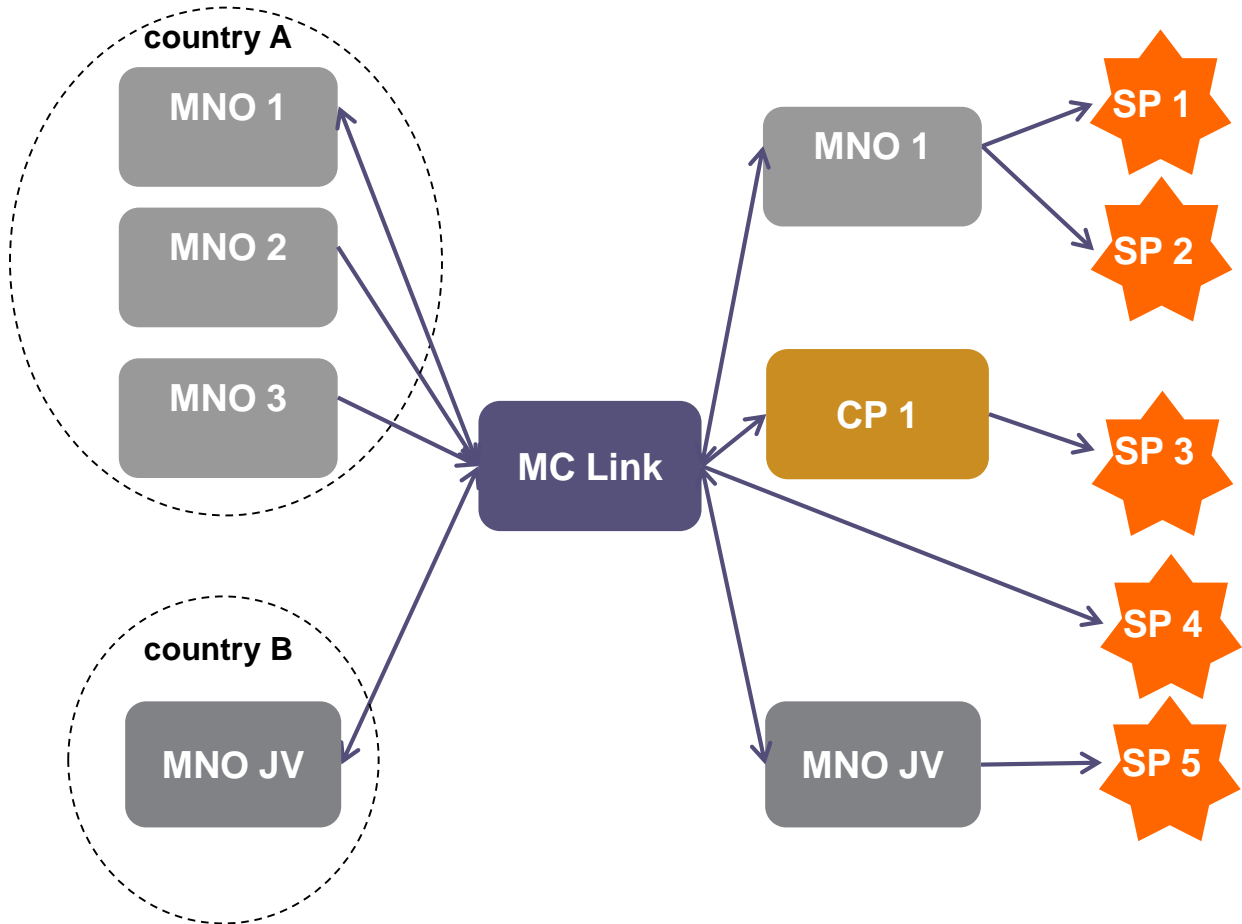
Finland: Circle of Trust between operators. Competition between MNOs to sell to SPs. Technical and commercial on-boarding on behalf of other MNOs. Inter-operator settlement. 1000+ SPs; 20,000 services

Norway: BankID is a JV between banks collaborating with MNOs. Common "BankID" branding. 100+ SPs
Canada: MNO JV offering MC pilot (3SPs). Each operator retains their branding
Taiwan: MNO JV to build and run a federated platform
Belgium: "ItsMe" JV together with banks

As an alternative or complement: GSMA offers MC Link to speed up commercial federation and allow any MNO to sell with full market coverage

Supply (end-user market coverage)

Demand (channels to market)



- GSMA is offering MC Link to operators as a trusted partner: MC Link acts as a neutral broker between the MNOs to **allow any MNO to sell MC with full market coverage**

- Effectively, MC Link provides wholesale regime between MNOs for enablement services, comparable to interconnect for voice and SMS

- Transparent criteria can be agreed to manage the business development in alignment with MNO strategy

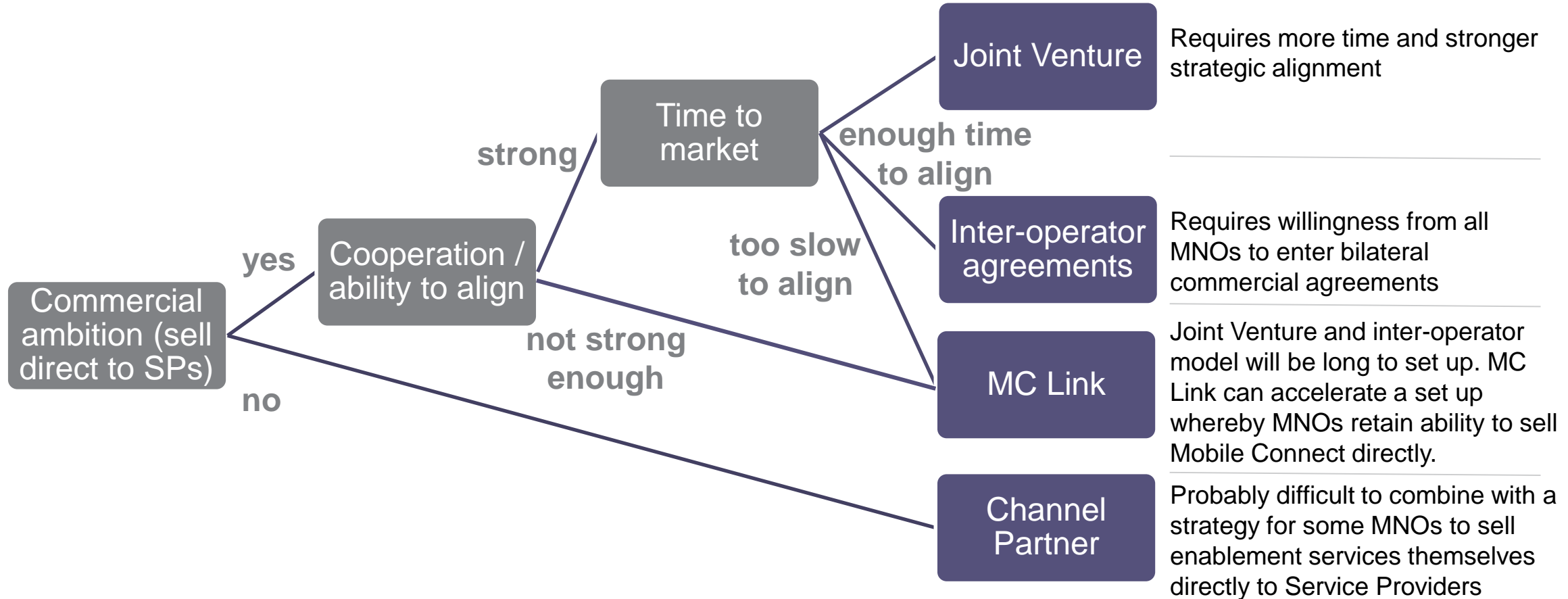
- Enabling a cooperative approach to **speed up x-MNO strategic alignment** (e.g. when inter-operator model is preferred but hard to reach)

- MC Link **opens up international reach** by providing access to global service providers using Mobile Connect and facilitating cross-border Mobile Connect services between MNOs

5 key questions will structure the Commercial Federation decision making process

1. What is the commercial ambition of each MNO?
Sell enablement services themselves directly to Service Providers or let others sell?
2. How strong is the cooperation on Mobile Connect?
Ability across MNOs to align strategically and enter commercial agreements
3. What is the required time to market to set up the commercial model?
4. Which model provides the best support for SPs?
5. Which models are possible under local competition law?

Answers to the key questions will guide the decision



This simplified decision tree is only a rough guide. In addition, MNOs will need to consider:

- Which model provides the best support for SPs?
- Which models are possible under local competition law?



Mobile Connect in Government applications
- Government sector update (worldwide) -

CONTENT

1. RECENT GOVERNMENTS ACTIVITIES & REGULATORY TRENDS
2. EXISTING MOBILE CONNECT PUBLIC USE-CASES
3. MOBILE CONNECT/EIDAS PILOT & RECOMMENDATIONS



The identity management system is evolving toward a ...



digital



Mobile



User-Centric model

Mobile ID on public services show extraordinary adoption rates

Iceland	
United Kingdom	
France	
Belgium	
Italy	
Spain	
Switzerland	



Mobile Connect
 Mobile ID
 Mobile Connect And Mobile ID

Norway	
Sweden	
Finland	
Estonia	
Lithuania	
Austria	
Moldova	
Turkey	

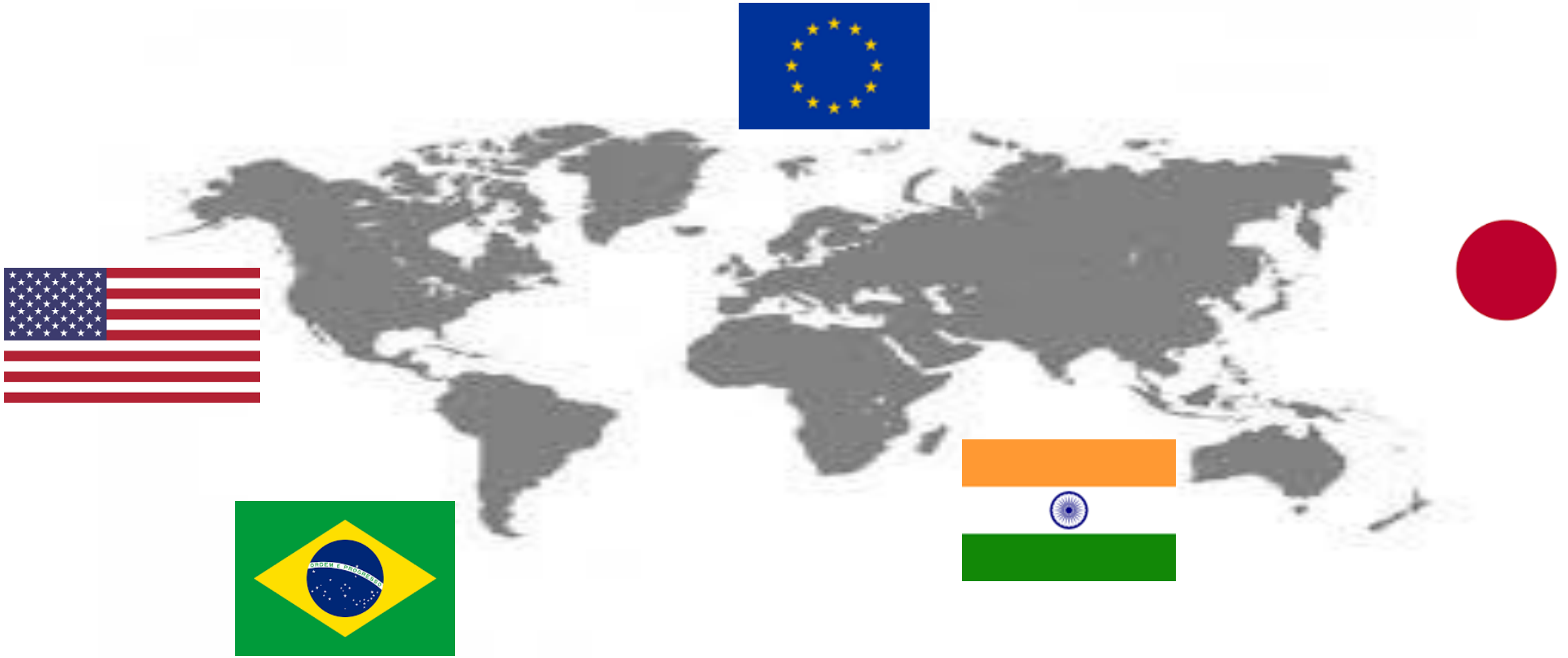
Member States mobile eID solution have shown extraordinary adoption rates. (Estonia; Austria)

Some private sector applications drive most of the usage on public services (Sweden and Norway with BankID).

The opening of Tax-on-web has caused an impressive 60% jump in new itsme mobile accounts. (Belgium)

Source: GSMA analysis February 2018

Latest Personal Data and Privacy Policy Revisions worldwide



Privacy by Design: Mobile Connect Privacy Principles

1. Openness, Transparency and Choice
2. Purpose and Use Limitations
3. User Choice and Control
4. Data Minimisation and Retention
5. Data Quality
6. Respect User Rights – Individual Participation
7. Security
8. Education
9. Children and Adolescents
10. Accountability

Will my personal information be shared with other people?

Your mobile provider won't pass on your mobile phone number unless you give your permission. When Mobile Connect does request additional information, for example, when you wish to make secure online payments, you can be reassured the information you disclose will only be used for the intended purpose.

New Identity players



GOV.UK Verify, user provides evidence (passport, bank, mobile phone account data) to a certified company, which then verifies their identity against different trustworthy public and private sector sources. Data are not stored centrally and there is no unnecessary sharing of information. As part of the UK's eGov initiative, the Government of the Channel Island of Jersey allow YOTI app to provide digital identity solution for government services, using a selfie to verify identity.



SPID allows various digital identities issued by private identity providers (Post-ID, TIM-ID etc) to access government services. All identity providers have been pre-notified to EU Member-States, and are under peer-review. First private national eID scheme to be notified under the eIDAS.



LOGIN.GOV, a single sign-on solution for government websites to access public services using the same username and password (two-factor authentication via mobile phones or authenticator application). All data are end-to-end encrypted and are not shared with partner agencies unless the user gives explicit permission.



GOVPASS, a digital single sign-on programme. User provides details from a number of personal documents (e.g. a birth certificate or driver's license), which are then verified by the government document issuer. Users upload a photo which is submitted for comparison with existing photo IDs. All submitted data and photos are deleted after verification is complete.



ITSME app (a consortium of banks and MNOs) to login to government services. A unique 5 digit code or fingerprint. ItsMe uses Government approved IDPs as the verified ID providers. The MNOs provide the security element and a SIM Applet for verification. Itsme does the commercial agreements with service providers and manages the association of the verified Identity provided by the Banks as the IDP and the MSISDN.



WECHAT app as national ID. Initial pilot in Guangzhou, limited functionality using the WeChat ID accessible through facial recognition alone, with full functionality granted after a user visits an offline station to physically validate paper ID cards.



AADHAAR, the largest biometric identity programme in the world with a unique 12-digit ID number, a photo and biometric data (fingerprints and iris scans). Also used to allow bank transactions and activating a mobile phone.



VERIMI, cross-industry identity and data service that helps manage personal data, single access point and lets see who you have authorized to access your data. In the future, digital administrative procedures and secure payments will also be possible and enable customers log in using video-identification process to authenticate identity cards and passports. Mobile Connect to be integrated to Verimi in 2018.

2. EXISTING MOBILE CONNECT PUBLIC USE-CASES





2. EXISTING MOBILE CONNECT PUBLIC USE-CASES



US – proof of concepts using Mobile Connect for authentication, identification and attribute verification (financial services, consumer goods, health, e-Government)



EU – eIDAS Pilot using Mobile Connect and eIDAS architecture.



UK – GOV.UK Verify, user provides evidence (passport, bank, mobile phone account data) to a certified company, which then verifies their identity against different trustworthy public and private sector sources. *Now fully commercially available.*

EU – CEF funded project on transferring identity cross-border to open bank account (eIDAS). Ongoing



CAT – Use of Mobile Connect to log into digital municipalities services in Catalonia. *Now live and expanding to other cities.*



TAIWAN – Government offers Mobile Connect as a digital identity solution to access a range of digital government services via pay.Taipei, also to access e-health and e-prescription. *Now live and expanding to new services.*



FR – Government allow access to the France Connect government services platform using Mobile Connect et Moi. *Live.*



DE – cross-industry identity and data service soon available for digital administrative procedures and secure payments. *Mobile Connect to be integrated to Verimi in 2018.*

Accessing France Connect public services portal using Mobile Connect et moi



1. Challenge and rationale

Public service providers are increasingly moving online to **make it easier** for citizens to complete processes and to reduce their administrative costs. However customer access is infrequent, making **credential management** difficult and leading to potential **security vulnerabilities**.

Public services also need to **verify and safeguard customer identities** in the digital space.

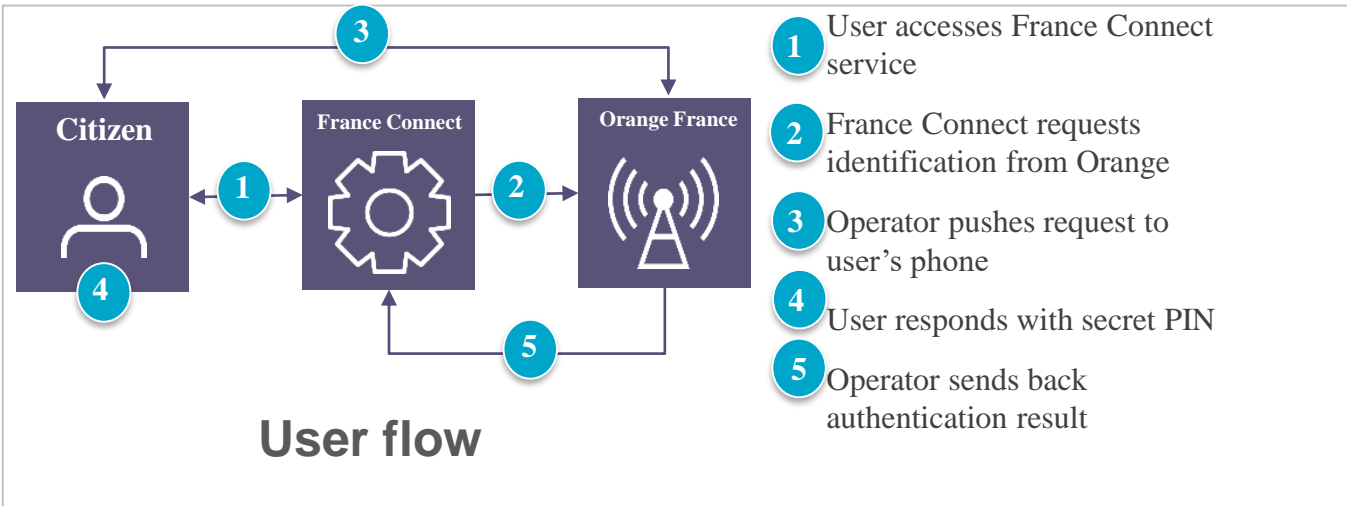
3. Benefits

- ❑ Removes the need for new username and password
- ❑ Quick, mobile-based registration and access, makes it possible to reach younger generations
- ❑ Mobile authentication offers high standards of security in line with upcoming eIDAS regulation
- ❑ Respects privacy – customer information is not shared without permission
- ❑ Mobile Operators increase user trust thanks to government endorsement

2. Solution

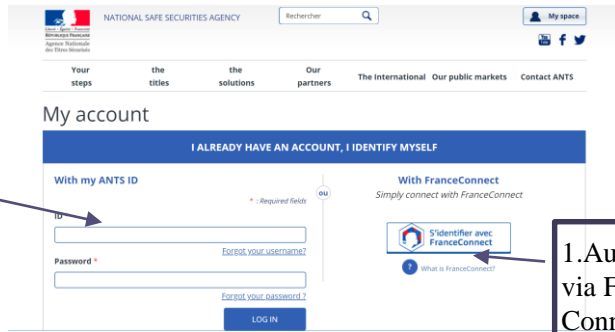
France Connect as an SSO to enable citizens to access an array of public services online. Orange France’s “Mobile Connect et Moi” is a trusted option allowing them to register and log-in with their mobile. Citizens’ identity is verified on registration by an identity provider using an ID document scan. They can then access all available public services using their mobile device and a secret PIN.

Used by 2,8 million users, 25 000 uses Mobile Connect et Moi to login. 1 000 more users/ week on average. Stable growth without marketing/communication. Still no commercial model agreed, pricing to be agreed end of June. MobileConnect et moi is now under evaluation by the ANSSI (French National Agency for Cyber Security). ANSSI to notify EU Member States about Mobile Connect as an eIDAS scheme for cross-border recognition end of 2018.

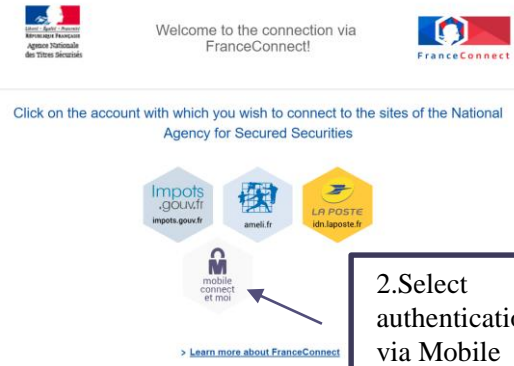


France Connect- Mobile Connect et moi account set up

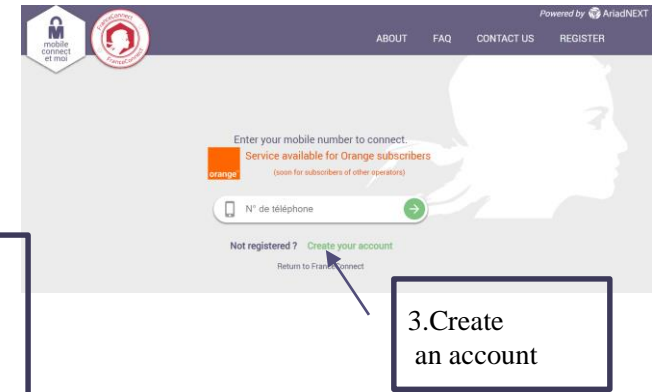
Standard Authentication to enter driving licence agency with user name and password



1. Authentication via France Connect



2. Select authentication via Mobile Connect et moi

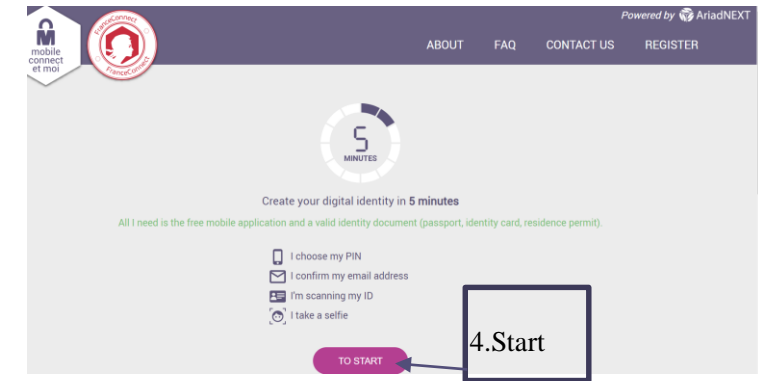


3. Create an account



- Mobile Connect Authentication (Or Mobile Connect account creation)
- email verification
- Official ID Scan (ex : passport) + on line data validation
- Security check : Photo & selfie accordance + liveness tests

5. MC and KYC enrolment process



4. Start

Accessing “Carpeta Ciudadana” on website of City of
Castellar del Vallés using an Orange phone number



Identifica't amb el mòbil

Document identificatiu

NIF ▾ 12345678A

Número de mòbil

003 669111222

Utilitza el meu idCAT-SMS

[Què és idCAT-SMS?](#) [Com em puc donar d'alta?](#)

L'ús d'aquest servei implica l'acceptació de les seves condicions d'ús

O altres sistemes

- Certificat digital:** DNIe, idCAT ...
- Cl@ve** PIN24, Ciutadans UE...
- Mobile Connect** +informació

[Ajuda](#) [Cancel·la sessió](#)

mobile connect

Comprobando tu identidad en Mobile Connect...

Has elegido acceder usando Mobile Connect

Asegúrate de tener tu móvil cerca y con cobertura para confirmar tu identidad.

□□□□□□□□

Mobile Connect le permite identificarte de forma segura y cómoda a través del mensaje de confirmación enviado a tu móvil.

Cancelar

Powered by

GSMA

Orange 08:32

Google

Servicios Orange

Autorizar el acceso a VALId Validador d Identitats.

Cancelar **Aceptar**

Google Cámara Play Store Ajustes

Orange 08:32

Google

Servicios Orange

Identificación correcta

Cancelar **Aceptar**

Google Cámara Play Store Ajustes

Ajuntament de Castellar del Vallès

Inici | Ajuda

Castellano | Català

Tràmits i gestions Roger Noguera Armau Desconnecta

Carpeta ciutadana

Les meves sol·licituds i expedients

Estat del tràmit Data del tràmit des de fins a

Cercar

Actuacions	Data de sol·licitud	Núm. de registre	Tràmit	Estat	Adjunts
	24/03/2016	E/000014-2016	Instància genèrica		PDF.pdf
	19/02/2016	E/000007-2016	Recollida de mobles i trastos vells al carrer		PDF.pdf
	19/02/2016	E/000006-2016	Queixes i suggeriments		PDF.pdf
	19/02/2016	E/000005-2016	Instància genèrica		PDF.pdf

[Ajuntament de CASTELLAR DEL VALLÈS. Tots els drets reservats.](#)
Servei prestat en col·laboració amb el Consorci AOC.

AOC Consorci d'Acció Local de Catalunya

3. MOBILE CONNECT/EIDAS PILOT & RECOMMENDATIONS



eIDAS and Mobile Connect cross-border pilot

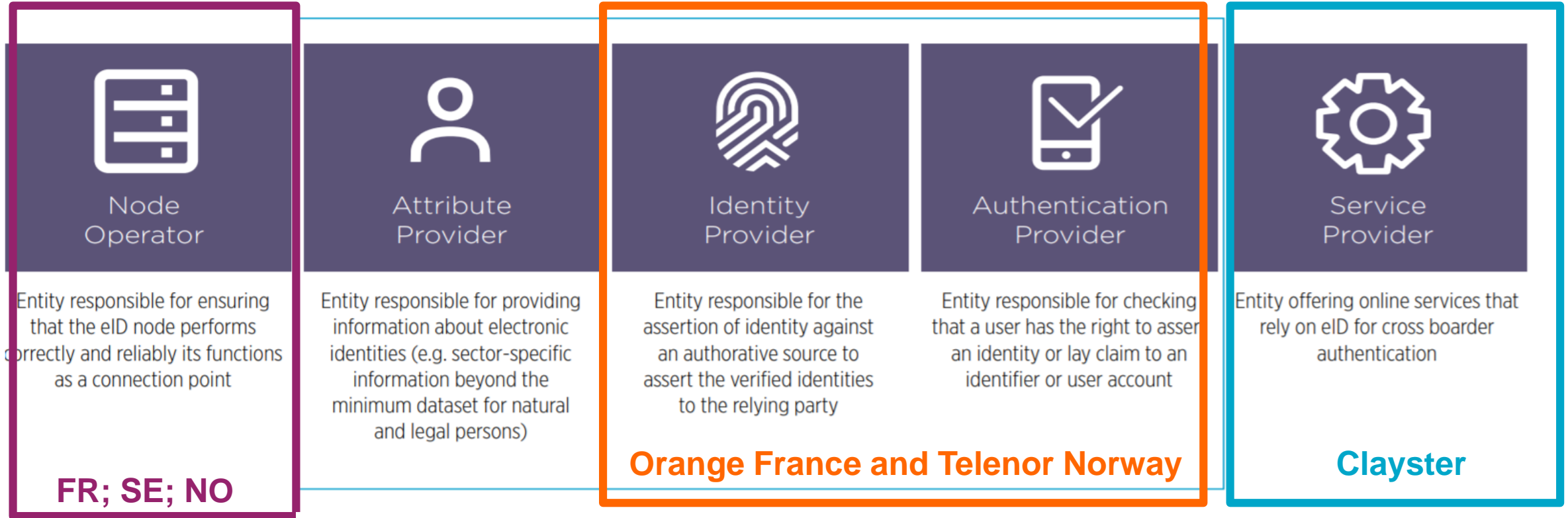
A multi-stakeholders public and private sector cooperation employing the requirements of a commercially viable, government backed solution, demonstrating how mobile operators can support via Mobile Connect the deployment and scaling of eIDAS within two or more European countries, positioning Mobile Connect as the first private-sector cross-border service authentication solution that meets the technical requirements of eIDAS.

Key outcomes

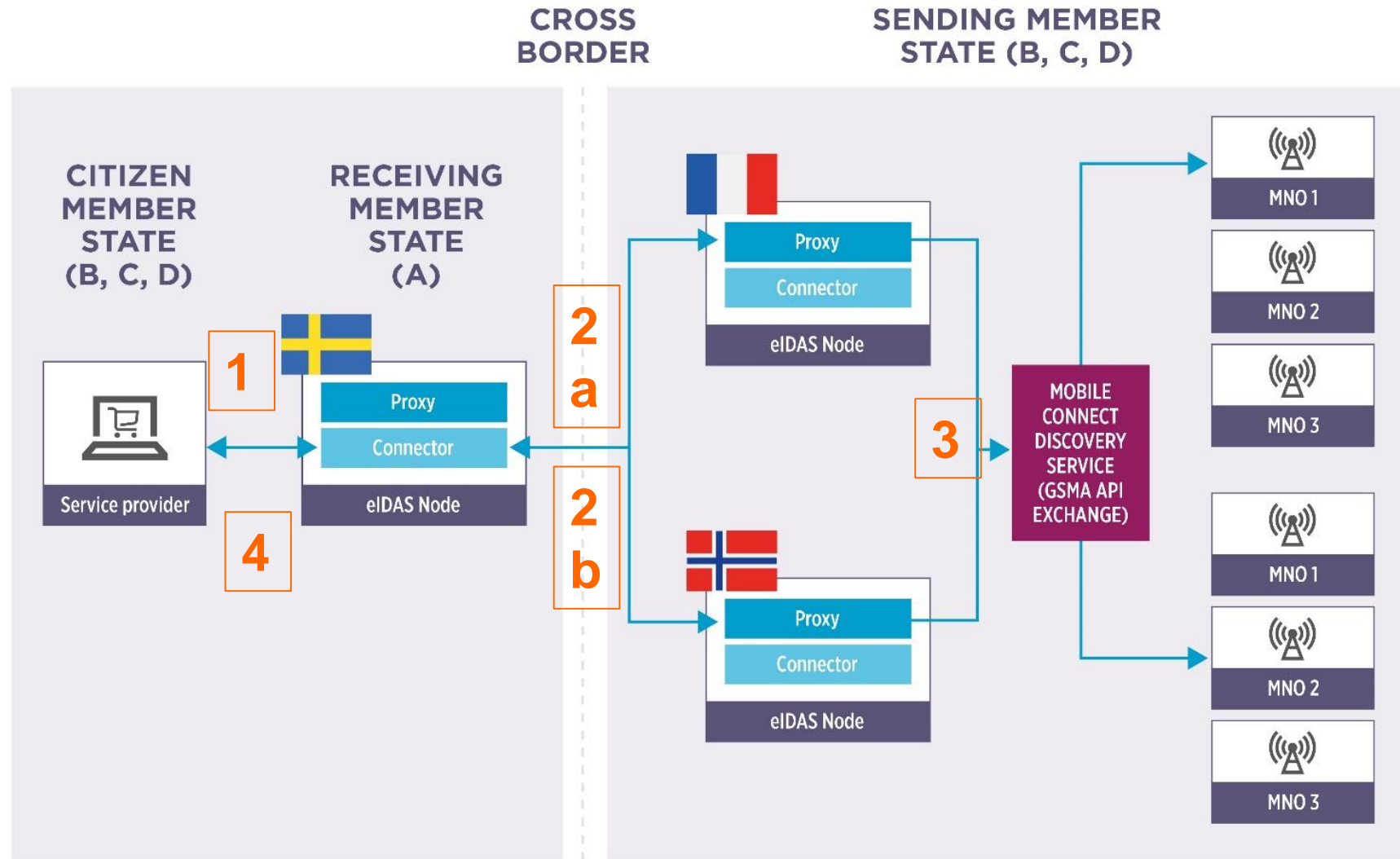
1. Deployed Mobile Connect authentication process and validation of the citizen's digital identity across France, Norway and Sweden using their eIDAS Framework.
2. Developed and tested the eIDAS Reference architecture #3 to demonstrate the interoperability of Mobile Connect and private sector service providers with eIDAS nodes integration requirements in a test environment.
3. Showcased a owner centric approach to test Mobile Connect secure authentication and eIDAS identity services to access healthcare private sector services in a Internet of Things application environment.



Role of the pilot participants



Trust Model



- Connector** One or more connectors per Member State (mandatory for mutual recognition of eID)
- Proxy** One Proxy-Service per Member State (optional component operated when the MS notified one or more eID schemes)

to Member States:

- i. **Pursue greater cooperation with the private sector**, in particular, to enable private sector identity and authentication providers to use the eIDAS infrastructure, thereby contributing to the emergence of an increased number of notified eID schemes with private sector stakeholders.
- ii. **Consult with industry on the chosen eIDAS architecture**, as its selection has important implications for the technical infrastructure deployed by private sector identity and authentication providers.
- iii. **Publish guidance to help companies to comply with each eIDAS Node's specifications**, including identity and authentication providers' service level specifications and service providers' on-boarding process.
- iv. **Standardisation of the interface exposed by the eIDAS Connector Nodes to the service providers via the OpenID Connect framework.**
- v. **Collaborate with the industry on the standardisation of domain specific attributes to be shared across borders**, including mapping of domain specific identifiers, on top of the identity layer established by the eIDAS minimum identity attributes.

To mobile operators and private sector service providers:

- i. **Foster and encourage the synergies between the government-verified identities (which can provide a high level of trust in the identification) and Mobile Connect** (which can provide a high level of trust and convenience in the authentication).

- ii. **The business model behind eIDAS requires further attention. Stakeholders should be consulted about a potential single contractual and commercial model, similar to the technical federation.** There is potentially great value in bringing a commercial model that works and allows for scale for all parties in the technical federation. One possible commercial solution could emerge from the ongoing work by the GSMA and several EU mobile operators in forming a commercial federation service called Mobile Connect Link (MC Link).



Mobile Connect for MVNOs



- This section explores the options for providing MC services by or on behalf of MVNOs¹ to deliver a higher percentage of user-base coverage within a target market²
- In doing so it discusses the different implementation topology choices based on MVNO type (MVNOs have been categorized into four main types – see next slide) and target MC services.
- In terms of deployment topology, there are two main options depending on whether the MVNO can be discoverable by the API Exchange (and hence provide MC services itself), or must rely on a host MNO to front MC services on the MVNO's behalf towards SPs
- This deck is focused primarily on the technical options with some considerations of associated commercial, contractual, branding, end user licensing and regulatory factors (although these factors will be largely market-dependent, they are important to assess in parallel to technical solutions).

¹ A Mobile Virtual Network Operator is effectively an entity that sells mobile connectivity services but does so by renting capacity from a licensed network operator (MNO) rather than operating its own network infrastructure - the MVNO will typically sign a wholesale agreement with the infrastructure owner (MNO) and set their own retail prices as per the market conditions.

² MVNOs typically represent 5-40% of the user base in developed markets

1. Reseller MVNO (Branded Reseller MVNO)

- Completely relies on host MNO's services and provisioning. Typically only differentiated by host MNO during the billing cycle.
- Might run sales and marketing operations. Can be owned by the MNO (i.e., a sub-brand)
- Users can be mapped to MVNO by host MNO

2. Light MVNO

- Takes ownership of customer support, marketing, sales and distribution
- Has billing operations and sets own tariffs independently
- Users can be mapped to MVNO by host MNO

3. VAS MVNO

- Strong brand control and customer loyalty
- Differentiation through Value-Added Services, content bundling etc.
- Users can be mapped to MVNO by host MNO

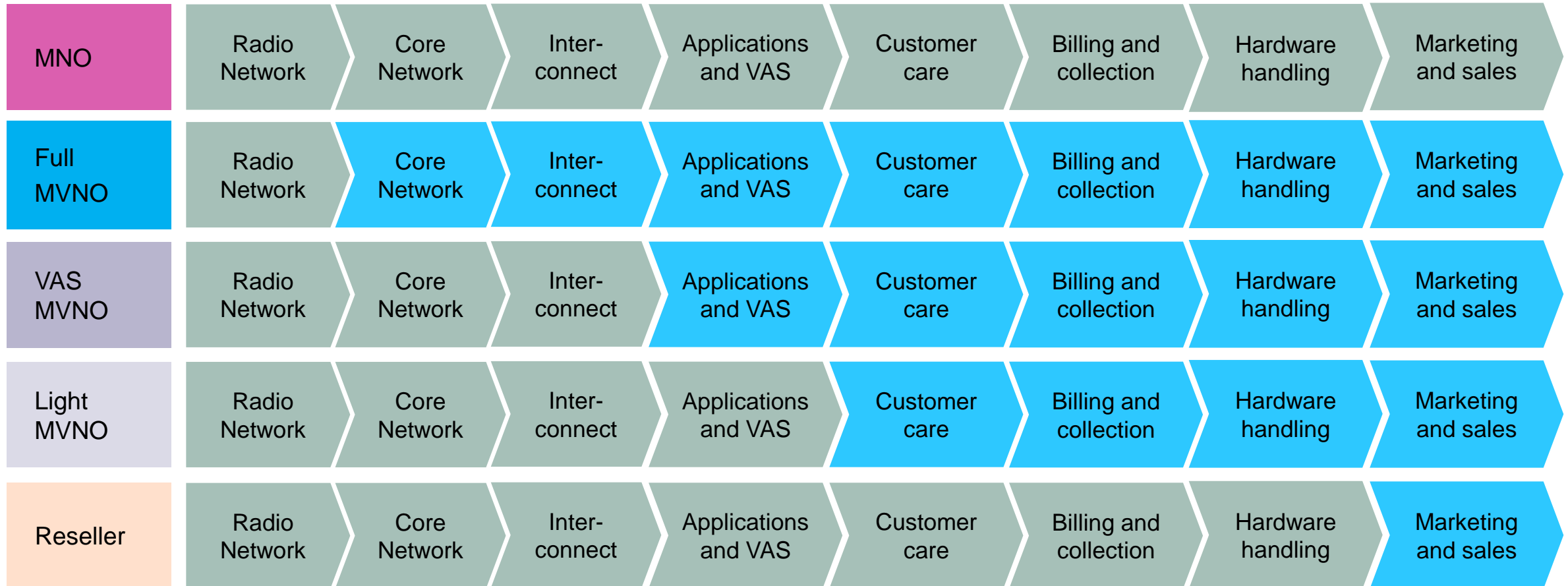
4. Full MVNO

- Acts as a full MNO, deploying own core infrastructure (has own MNC network identifier) but wholesales the radio access network from one or more MNOs
- Users can be mapped to MNO by discovery node

Note #1: Aggregators (MVNA) and Enabler entities (MVNE) will be considered separately as needed

Note #2: In addition to presented MVNO types, there are many hybrid MVNOs who are only partially fulfilling some of the roles and functions.

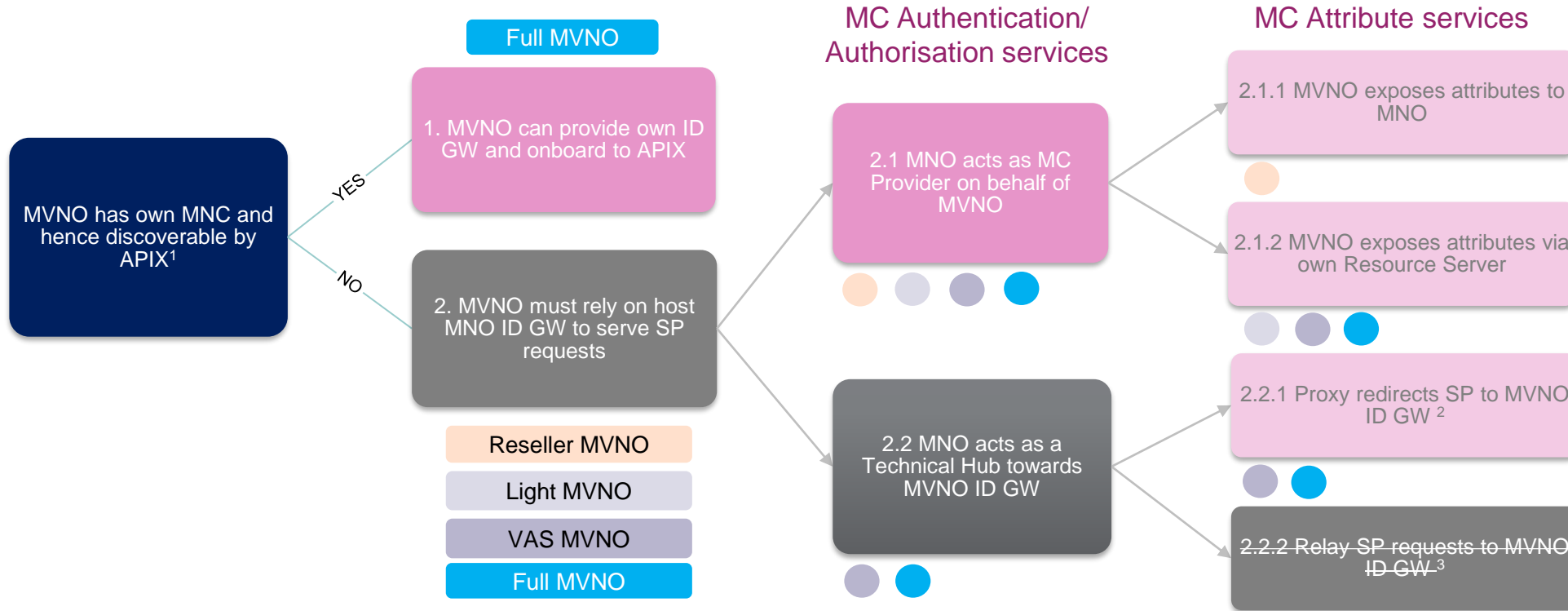
MVNO roles/functions per type



Topology options & decision tree

Recommended

Candidate



¹ APIX uses MNC for distinguishing between Serving MNOs and responding to the SP with the correct ID GW details; only a Full MVNO with own core infrastructure will have an MNC and be able to provide a GGSN IP address range for APIX to use in identifying the correct mobile network; in situations where a market has deployed a Local Discovery Node, MVNO users may be discoverable via other means. Although dependent on MVNO number range including ported numbers being known to the Pathfinder service

² Development and integration becomes more complicated, deviates from standard MC architecture and adds additional burden on service provider - hence not recommended.

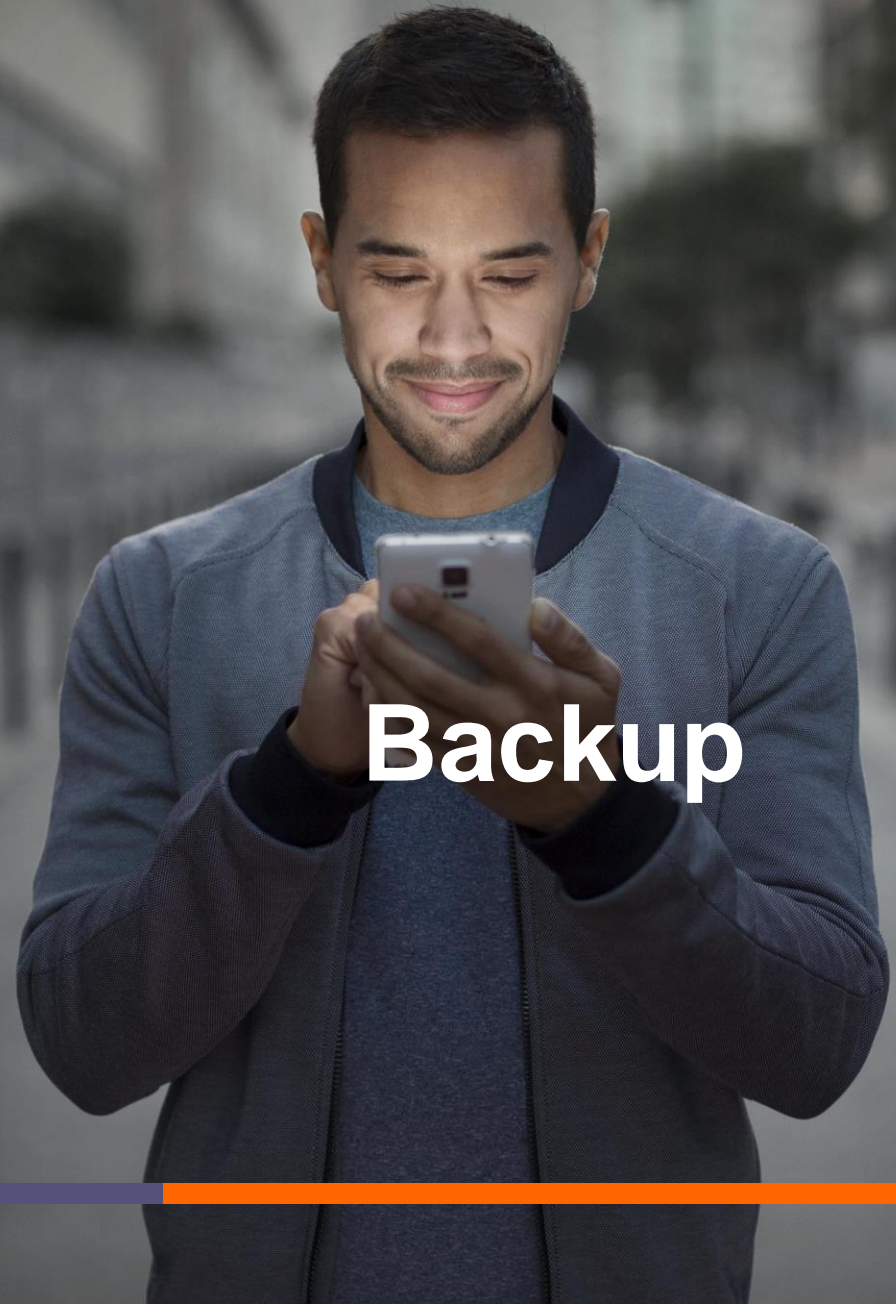
³ A Relay approach could be used but would be limited in the case of MC Identity/Attribute services due to MVNO data flowing through the host MNO (privacy consideration), will complicate discovery process, server initiated mode will be required, product offering might be restricted and SP access control becomes complicated, requires multiple discovery requests. - hence has been discounted from the candidate options

Summary of commercial options/considerations

	1. MVNO can provide own ID GW onboard to APIX	2. MVNO must rely on host MNO ID GW to serve SP requests	
		2.1 MNO acts as MC Provider on behalf of MVNO	2.2 MNO acts as a Technical Hub towards MVNO ID GW
Provider of Mobile Connect services	MVNO can deploy own solution	MVNO contracts with host MNO for provision of service on their behalf	MVNO can deploy own solution, but will need an appropriate Technical Hub contract with MNO
Brand displayed to MVNO's users	MVNO can present Mobile Connect under own brand	Can host MNO ID GW discern users of MVNO? <ul style="list-style-type: none"> • Yes – Can show MVNO brand • No – Can only show MNO brand 	MVNO can present Mobile Connect under own brand
End user license agreement (EULA) for MVNO's users	MVNO can serve own users	Can host MNO ID GW discern users of MVNO? <ul style="list-style-type: none"> • Yes – MNO can provide users with MVNO EULA • No – MC can be included as part of general EULA by MNO/MVNO but if the aim is to sign-up users on the fly then only the MNO EULA can be provided 	MVNO serving own users hence can provide EULA

Discussion & closing remarks





Backup



Commercial Federation: Detailed benefits and drawbacks of each model

Models	Pros	Cons
1. Direct Sales	Aligns commercial and technical architectures	<ul style="list-style-type: none"> • Multiple sales points for SP • Each MNO needs to invest in sales • Does not scale
2. Channel Partner	<ul style="list-style-type: none"> • Time to market • Known model (carrier billing, wholesale SMS...) • Partners know how to add value / integrate in SP business 	<ul style="list-style-type: none"> • Margin loss • Lack of strategic control and no influence on the end-SP e.g. re user experience • MNOs may not be able to sell to SP directly in parallel • Hard / impossible for MNO to enter into resell agreement with channel partners if MNO wants to sell MC directly • Limited number of partners
3. Lead Operator	Single point of sales to global SP for whole market	<ul style="list-style-type: none"> • Only the Lead Operator can sell to SP • Complexity in setting up the inter-operator commercial agreements
4. Joint Venture (JV)	Should enable strategic alignment between JV and operators	<ul style="list-style-type: none"> • High strategic alignment required between MNOs • Costly and long to set up if not existing already • Complex governance model; potential conflicts of interest
5. Inter-Operator	<ul style="list-style-type: none"> • Easy for additional MNO to join • All MNOs can take part in selling to SP – encourages competition • Alternative SP sales strategies from minimal sales effort to SP sales focus – margin dependent on SP sales effort 	<ul style="list-style-type: none"> • Complexity in setting up the inter-operator commercial agreements; requires a strong foundation of trust between MNOs • Time consuming (>12months) and high likelihood for delays and/or failure due to breakdown in negotiations
6. MC Link	<ul style="list-style-type: none"> • Trusted partner, allows the MNOS a strategic choice of where to play in the value chain: suppliers and resellers if they want, with full market coverage, or only suppliers • Opens up international reach 	<ul style="list-style-type: none"> • Broker model, still requires effective channels to market for commercial success • Operators need to contract with a UK-based entity

MVNO Summary & recommendations

- Full MVNOs **Full MVNO**
 - Will have own core infrastructure and MNC so will be able to deploy own MC infrastructure as well as having a choice of a range of authenticator options [\[model 1\]](#)
 - ...although has option of going for host MNO ID GW (with potentially own authenticators and resource server)
- VAS MVNO **VAS MVNO**
 - Typically have existing service infrastructure (VAS) hence could deploy MC infrastructure itself (incl. SAA authenticator), as well as using as login for own VAS services [\[model 2.2.1\]](#)
 - ...but would be dependent on host MNO acting as Proxy hence complicating service delivery & operation and requiring SP to support the API integration accordingly - see separate ppt on Technical Hubs for more discussion
 - ...doable option but not recommended
 - Alternatively VAS MVNO could utilise host MNO ID GW but still control authentication via own SAA and/or deploy own Resource Server for attribute services [\[model 2.1.2\]](#)
 - ...or could follow same path as for Light/Reseller MVNOs...
- Light/Reseller MVNO **Light MVNO** **Reseller MVNO**
 - Have no service-delivery infrastructure hence would most likely need to outsource MC service provision/operation to host MNO [\[model 2.1.1\]](#)
 - Suitable for MC Authenticate/Authorise services
 - Possibly OK for Network Attribute services (ATP, VM)
 - Needs evaluation for Identity services where MVNO would need to provide user information to the host MNO unless the MNO is already managing CRM anyway on behalf of the MVNO (i.e., Reseller MVNO)
 - Raises broader range of considerations around privacy, data protection, competition and trade secrets.
 - In all scenarios of host MNO ID GW being part of the MC product delivery flow, discovery of end user's MVNO is to be considered and agreed [\[model 2\]](#)
 - Impacts branding and end user license agreement
 - Can have contracting, legal and regulatory implications.

The impact of MVNAs and MVNEs within a market and the additional topology options that might be feasible will be considered when reviewing the specific circumstances within a given market