



RUSSIA & CIS
MOSCOW • 30-31 OCT 2018

Workshop «Digital Identity»

31 October 2018, Four Seasons Moscow

RUSSIA & CIS

MOSCOW • 30-31 OCT 2018

- **09:00 - 09:05.** Workshop opening
- **09:05 - 09:20.** Welcome speech by RCC
- **09:20 – 10:20.** Mobile Connect introduction
 - Introduction and global coverage – Tair Ismailov (GSMA)
 - Vedomosti Pilot presentation – Alexey Vasiliev (Tele2)
 - MegaFon's Mobile Connect research outcomes – Kirill Samoshonkov (MegaLabs)
 - Operators' plans for Mobile Connect introduction in Russia – Ilya Nestor (MTS)
- **10:20 – 10:35.** Coffee-break
- **10:35 - 11:40.** International experience of using the Mobile Connect solution for government services
 - Orange France experience with Mobile Connect et moi – Serge Llorente, (Orange France)
 - European eIDAS integration with Mobile Connect– Laszlo Toth (GSMA)
- **11:40-12:50.** Open discussion «Ways of improving the regulation of identification procedures within regional Digital Economy programs» (Moderator: Arsen Balasanyan, Tele2)
- **12:50 – 13:00.** Workshop wrap up
- **13:00 – 14:00.** Lunch at the Mobile 360 Russia & CIS event



MOBILE
360
SERIES

RUSSIA & CIS
MOSCOW • 30-31 OCT 2018

Mobile Connect introduction

- Introduction and global coverage – Tair Ismailov (GSMA)
- Vedomosti Pilot presentation – Alexey Vasiliev (Tele2)
- MegaFon's Mobile Connect research outcomes – Kirill Samoshonkov (MegaLabs)
- Operators' plans for Mobile Connect introduction in Russia – Ilya Nestor (MTS)

Secure access to digital services



Single mobile operator identity solution for online services



Identification by phone number



Secure personal data sharing and operations through secure Operator's channels

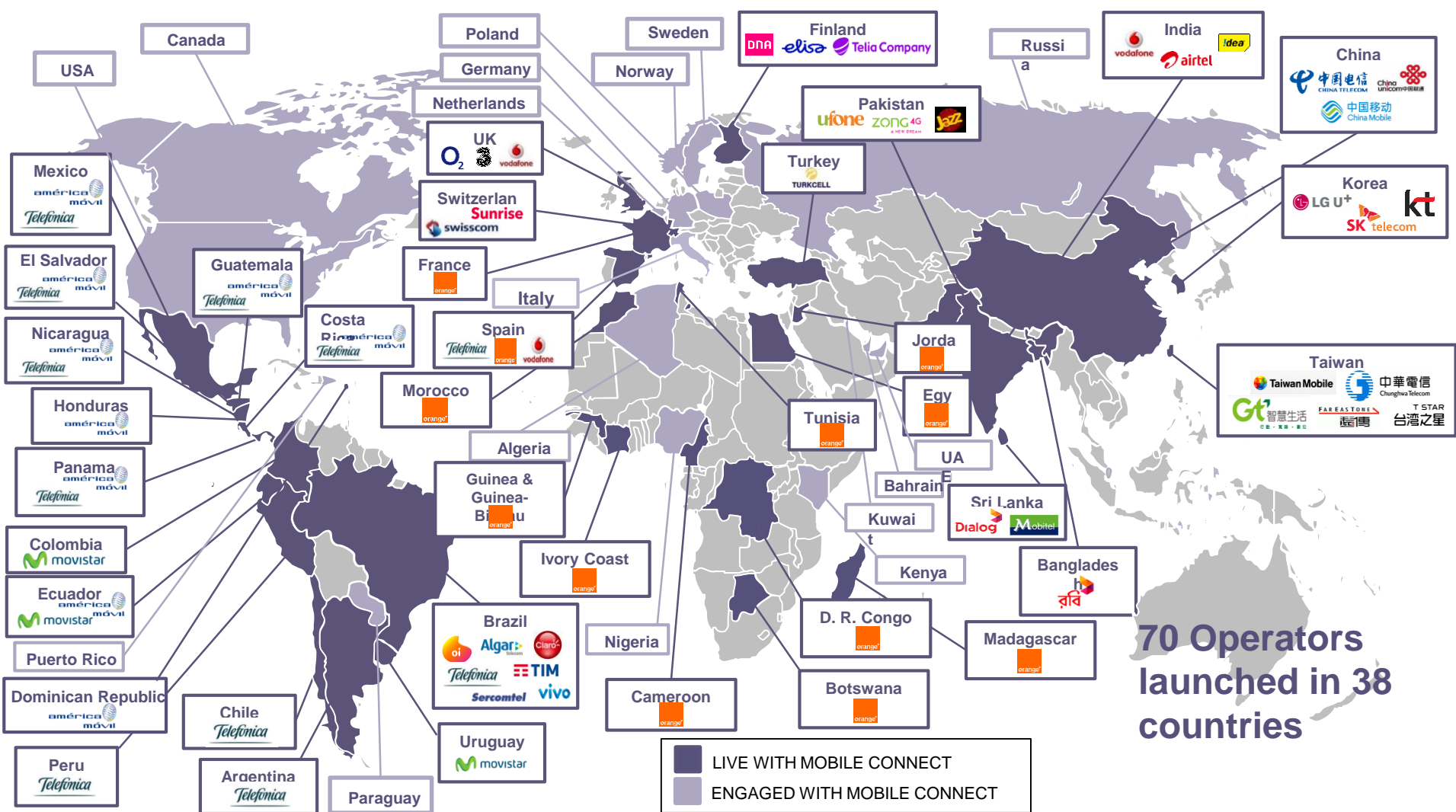


Password-less login to online resources across any device (mobile, tablet, laptop)

88%

of consumers say a single secure login solution would be beneficial to them

Sources: GSMA Consumer Research 2015, Cyber Streetwise



Use case examples



E-commerce:

Eliminates log-in friction, ensures less abandoned transactions and drives repeat business, reducing risk of data breach and fraud



Travel & Hospitality:

Leveraging mobile for e-ticketing, mobile identification, internal employee on-boarding and loyalty schemes



Banking:

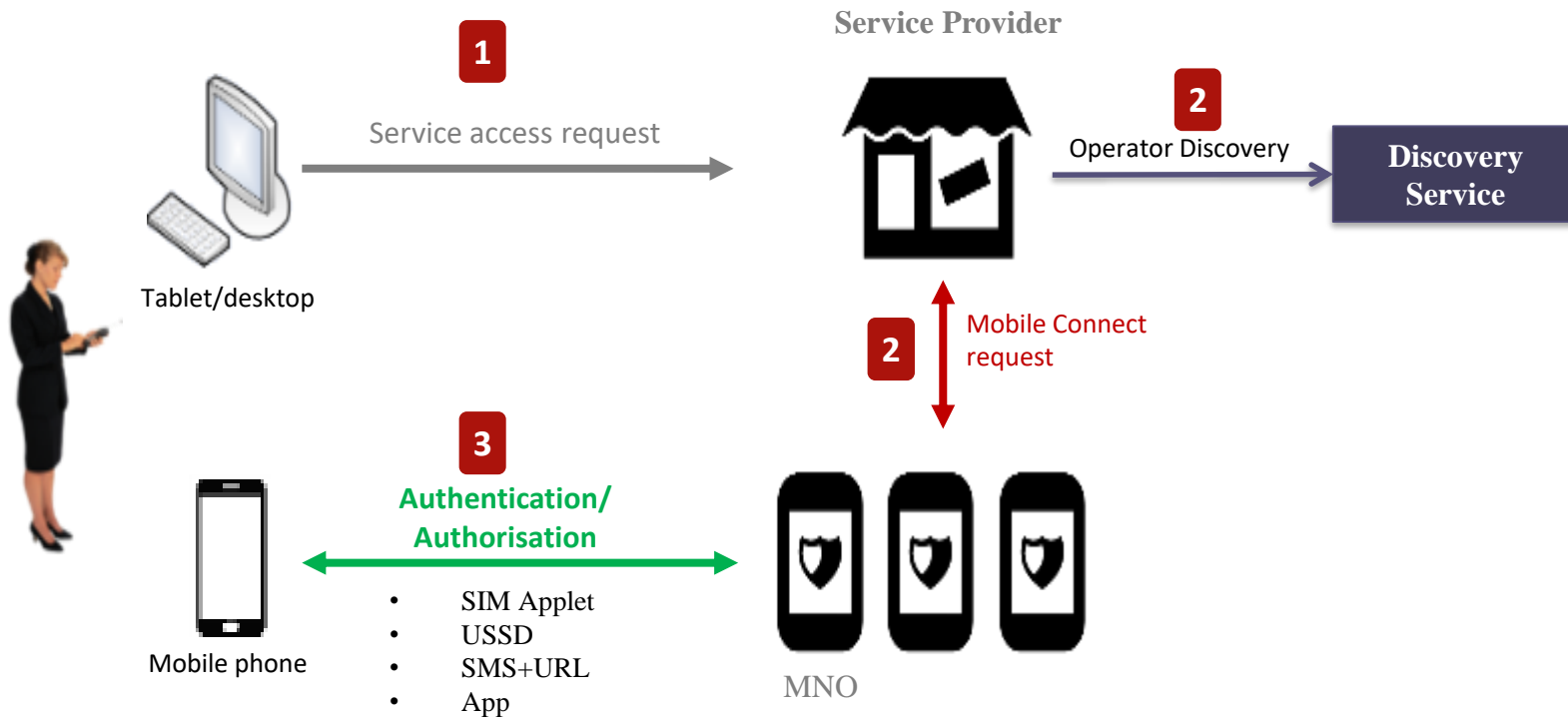
Enhancing the security of online banking by authenticating access and authorising online payments

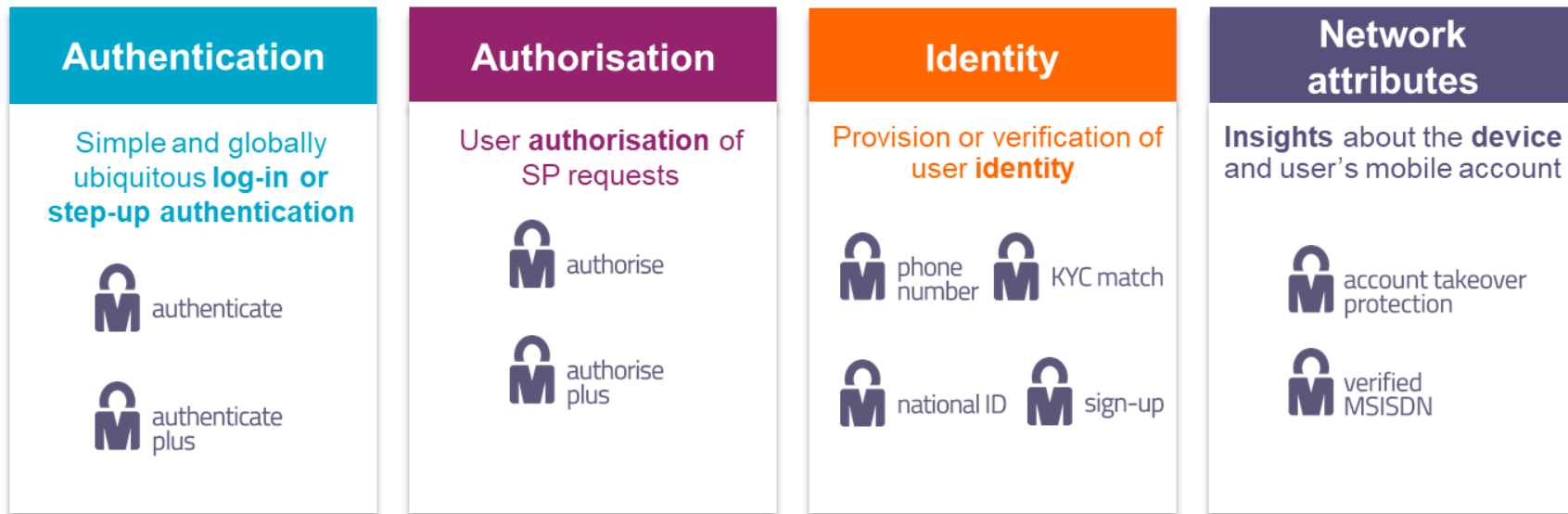


Government:

Simple citizen and employee log-in to eGovernment services
e.g. healthcare, education, smart cities and voting

How it works?





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

Simple and secure user authentication on a global scale

How it works?



**AUTHENTICATION
REQUESTED**






**USER
CHALLENGED**



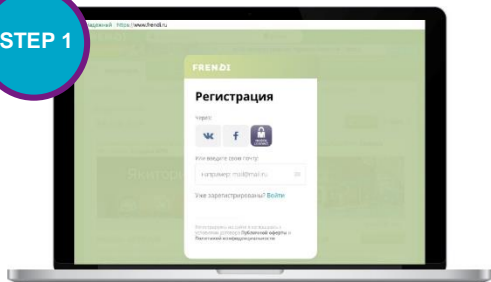
**ACCESS
GRANTED**

Use cases

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

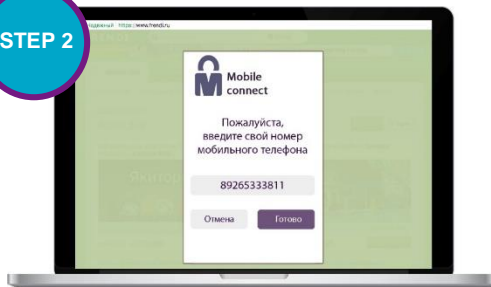
Use Case 1: Fast login (authentication by SIM applet push)

STEP 1



User accessing the website and selects the method of logging / registering using Mobile Connect

STEP 2

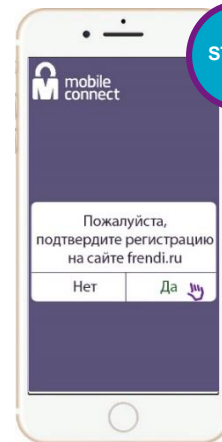


User gets a window with a field for entering a phone number.

WEB-resources providing content / services for registration and authorization

Online shops, online services, media resources, etc.

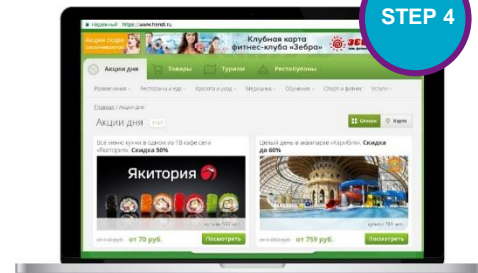
STEP 3



User receives a SIM applet push message to the phone.

User confirms the registration / login on the website.

STEP 4



Login / Registration is complete. User is redirected to the requested page of the website.

Simplifying customer authentication

Mobile Connect as a log-in option on M-Pesa



July 2016

Mobile Connect
launched in India

600m

Enabled users

M-Pesa

Is among the first
service providers
integrated

BEFORE MOBILE CONNECT

- Use SMS-OTP to log-in to accounts
- 8-step process, juggling between apps on a mobile
- Results in a cumbersome user experience

AFTER MOBILE CONNECT

- 1-click authentication on mobile data
- User flow reduced to 3 steps over Wi-Fi: enter mobile number, respond "1" on USSD prompt and confirm
- Binding to the mobile device is preserved



Results

+162% transaction
volume on M-Pesa
using Mobile
Connect in Q4 2016

Customers say
**"The flow is too
quick!"**
on the mobile data
network

Contextual & explicit approval through a mobile device

How it works?



**REQUEST
INITIATED**






**AUTHORIZATION
APPROVED**



**TRANSACTION
COMPLETED**

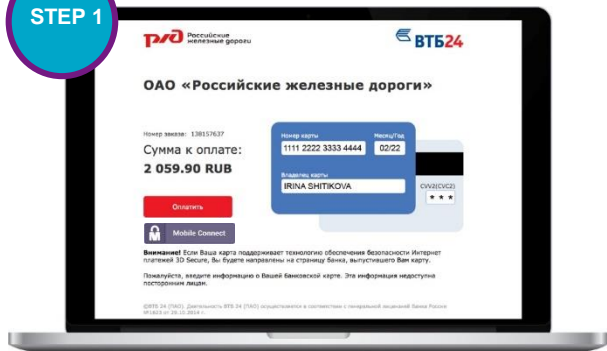
Use cases

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

Use Case 2: Authorization (2-factor)

Banks, all services that have online accounts and operations that require an increased guarantee of personal identity

STEP 1



User makes a purchase on the website and selects the method of payment online.

The bank knows that the user is connected to the MC and asks to confirm their operation with their PIN on the phone

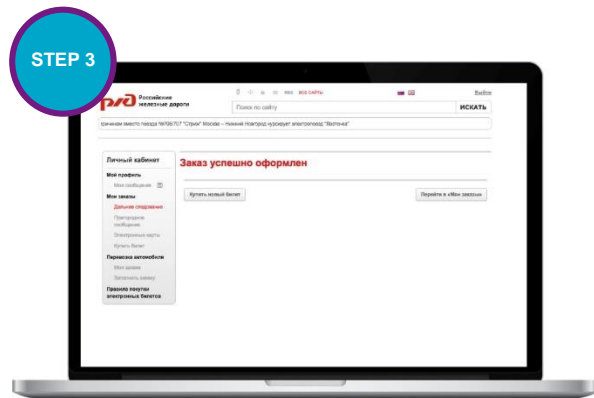
STEP 2



User enters their pin.

Trustee - Operator - confirms the accuracy of the data

STEP 3



User receives approval from the bank.

Purchase completed

Verified personal data retrieval with user consent

How it works?



**IDENTITY
REQUESTED**






**CONSENT
ACQUIRED**



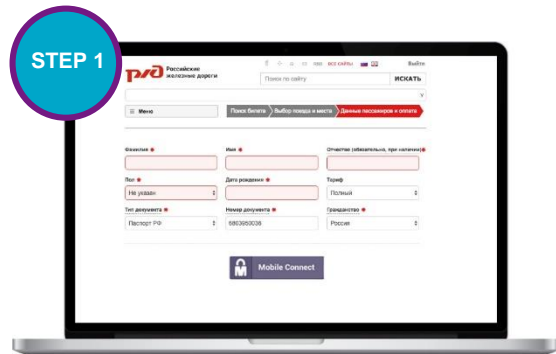
**USER DATA
SHARED**

Use cases

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

Use Case 3: Form filling

State companies, public services portals, digital services.
All online services where knowledge of the user's personal data is necessary
for the provision of services

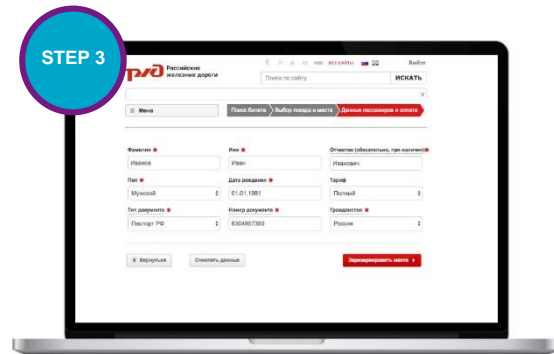


User must provide their data for purchase on the website.

User chooses to transfer their data to the website using MC



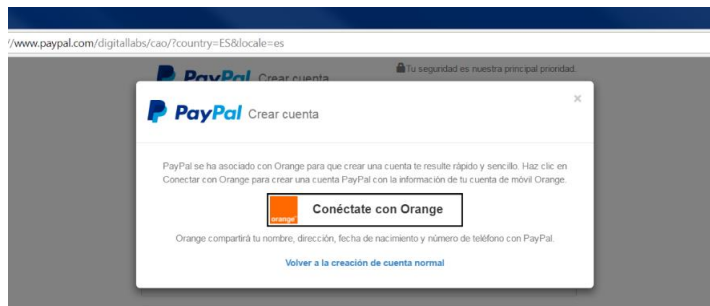
User receives an invitation on the phone to confirm the transfer of data and enter their PIN.



All requested data is transferred to the website.

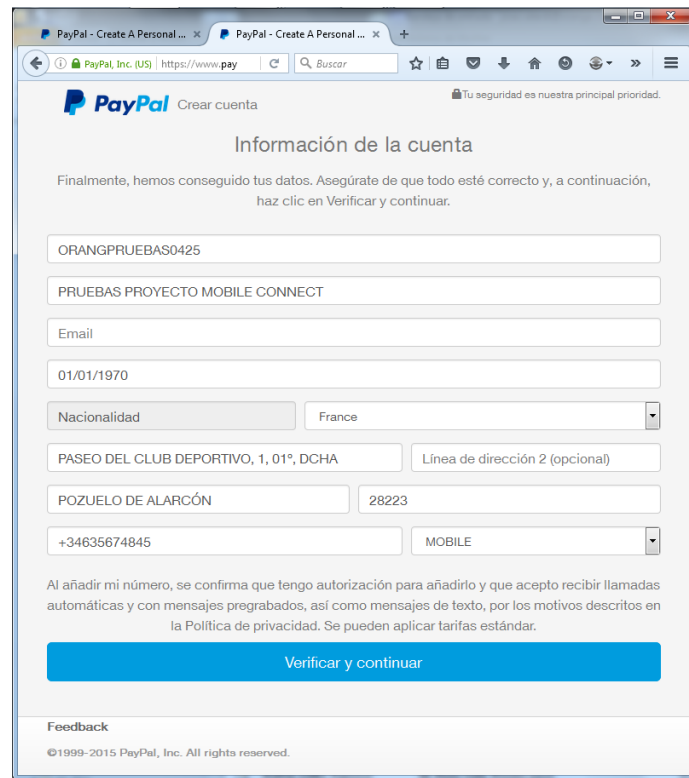
PayPal – Mobile Connect Sign Up (Identity services) in France-Spain

1



2

3



4

Mobile subscriber checks for ID verification & fraud mitigation

How it works?



**INTELLIGENCE
REQUESTED**






**NETWORK CHECK
DONE**




**RESULTS
SHARED**

Use cases

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

Global use cases for government services 1/2

<p>France</p> <p>Mobile Connect & Moi</p>  <p>S'identifier avec FranceConnect</p> <p>Qu'est-ce que FranceConnect?</p>	<p>“Mobile Connect et Moi”, the solution provided by Orange to allow French citizens register and log in to the single public services portal using a phone number.</p>	<p>https://www.impots.gouv.fr https://www.ameli.fr https://www.laposte.fr</p>
<p>Switzerland, Norway, Finland, Sweden, Estonia</p> <p>Mobile ID</p> <p>Bank ID</p>	<p>Mobile ID is used not only to access government, social, and banking services, but also as a digital signature and identification tool.</p> <p>Bank ID - a single identification tool for banking transactions and use of banking services</p>	<p>https://www.norge.no/en/electronic-id https://www.skatteverket.se https://www.bankid.com/en/ https://www.swisscom.ch https://e-estonia.com https://mobiiilivarmenne.fi/eng/</p>
<p>Taiwan</p> <p>payTaipei based on Mobile Connect</p>	<p>The Mobile Connect based payTaipei solution is used for authorization in government services using a phone number</p>	<p>https://pay.taipei</p> <p>http://english.doit.gov.taipei/News_Content.aspx?n=02BE20A482B22567&sms=DFFA119D1FD5602C&s=61A12A7EBE603B5E</p>

UK KYC match based on Mobile Connect	Government organizations use Mobile Connect based KYC match to verify operator's user data when accessing government services	NA
Spain Mobile Connect	Residents of three cities in Catalonia can use the city services portal using Mobile Connect solution in conjunction with an electronic identifier	http://web.gencat.cat/en/actualitat/detall/Mobile-Connect



**MOBILE
360
SERIES**

RUSSIA & CIS
MOSCOW • 30-31 OCT 2018

Vedomosti pilot presentation

Alexey Vasiliev, Tele2

Vedomosti daily is a unique project, brought to life in 1999 by two leading global business newspapers, Financial Times and The Wall Street Journal.

Online subscription allows to get:

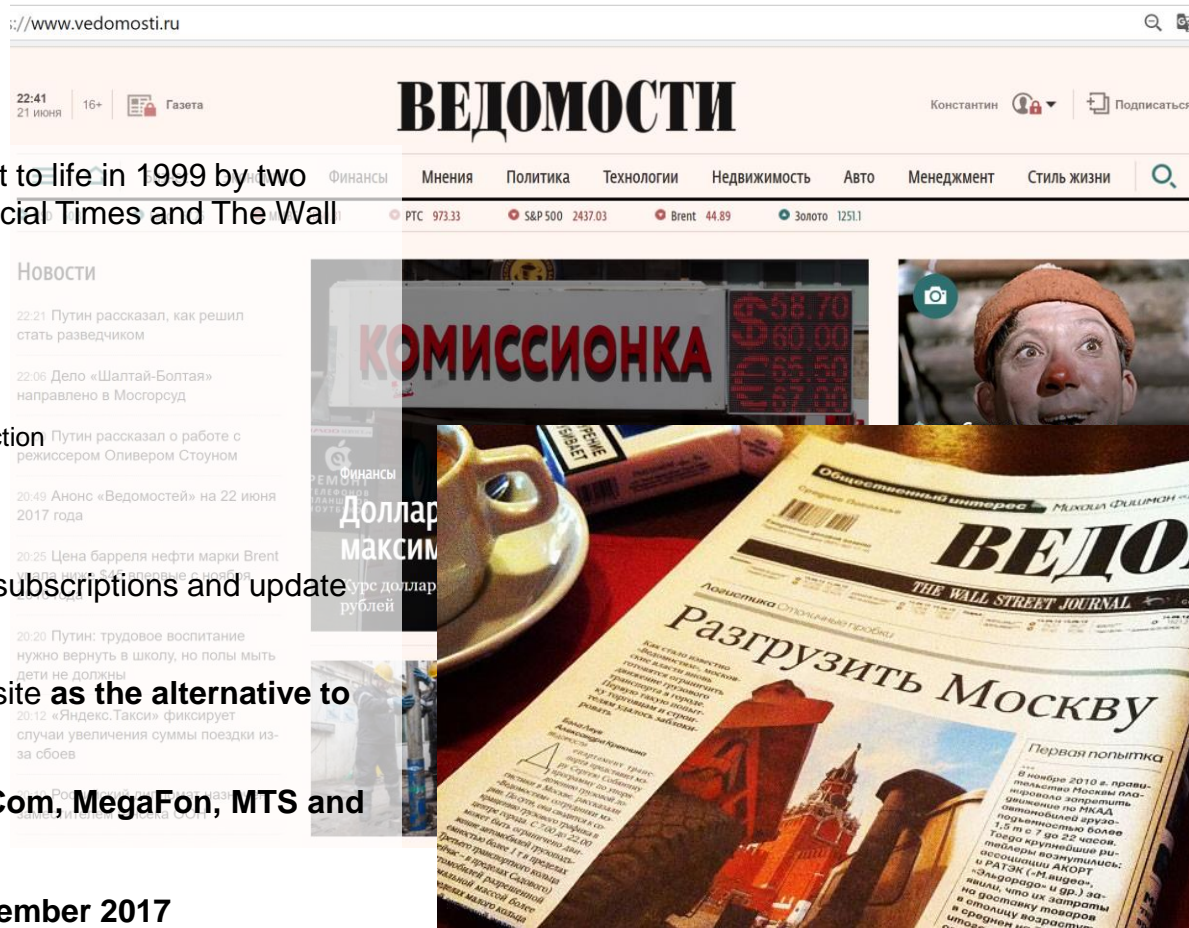
- Access to all news on all devices and the app
- Latest issue under «Today's Newspaper» section
- Daily newsletter with «Today's Newspaper»
- Capability to comment articles

In the self-service users can manage their subscriptions and update their data

Mobile Connect is used on Vedomosti website as the alternative to self-service login with password

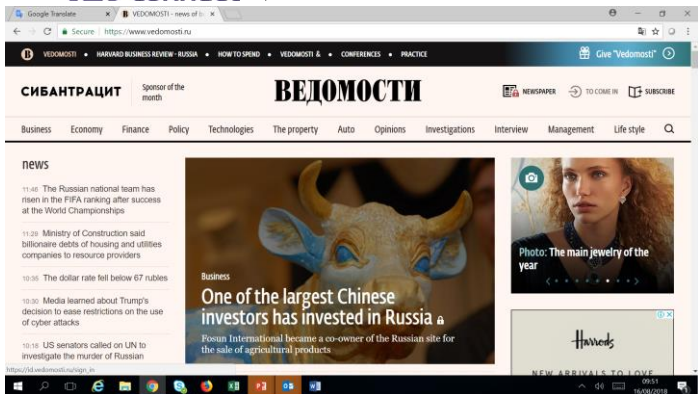
Operators participated in the pilot: **VimpelCom, MegaFon, MTS and Tele2**

Pilot launched on public website since **December 2017**

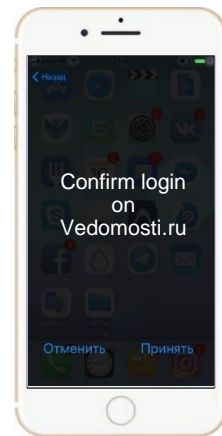
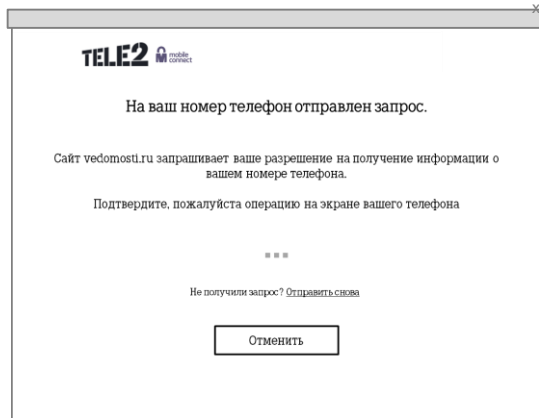
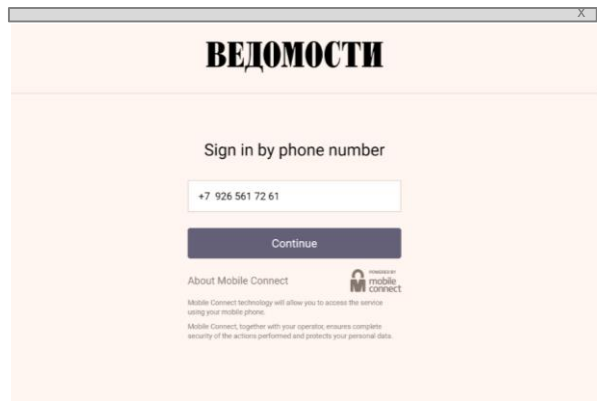
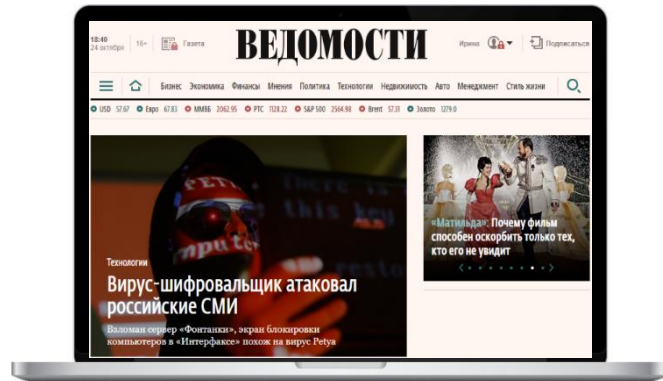




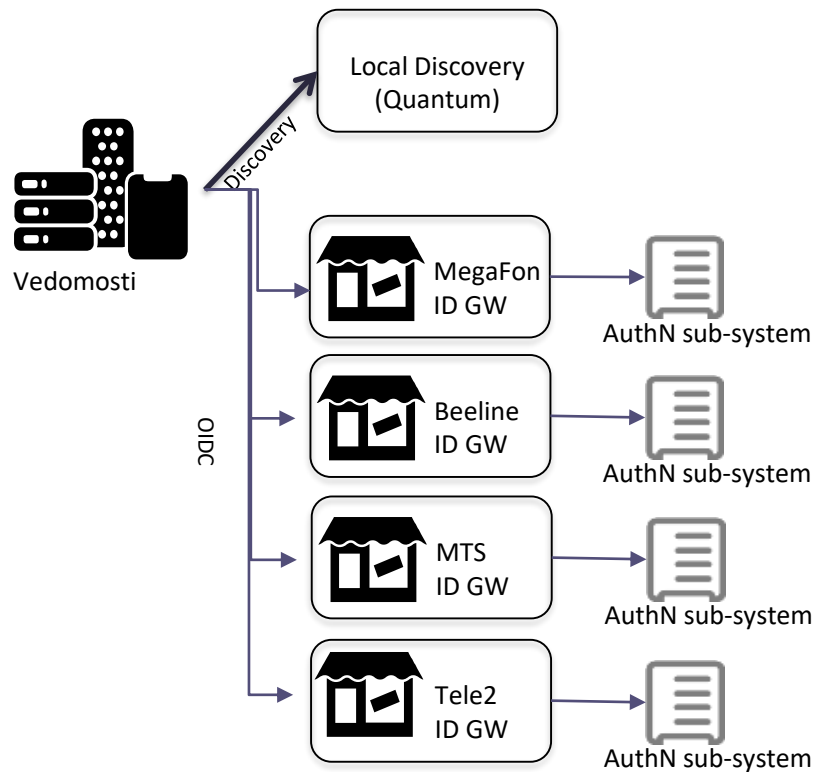
Login and new registration on Vedomosti's website with Mobile Connect (fast login with phone number)



- According to the results of the pilot logins via MC are more preferred than via local social network VK.
- For new users, the way to login with the phone number is already becoming preferred.



Technical scheme





MegaFon's Mobile Connect research outcomes, Kirill Samoshonkov (MegaLabs)



MOBILE CONNECT

Customer perception study

1

B2C

QUALITATIVE RESEARCH



MOBILE CONNECT FEATURES STUDY



Objectives

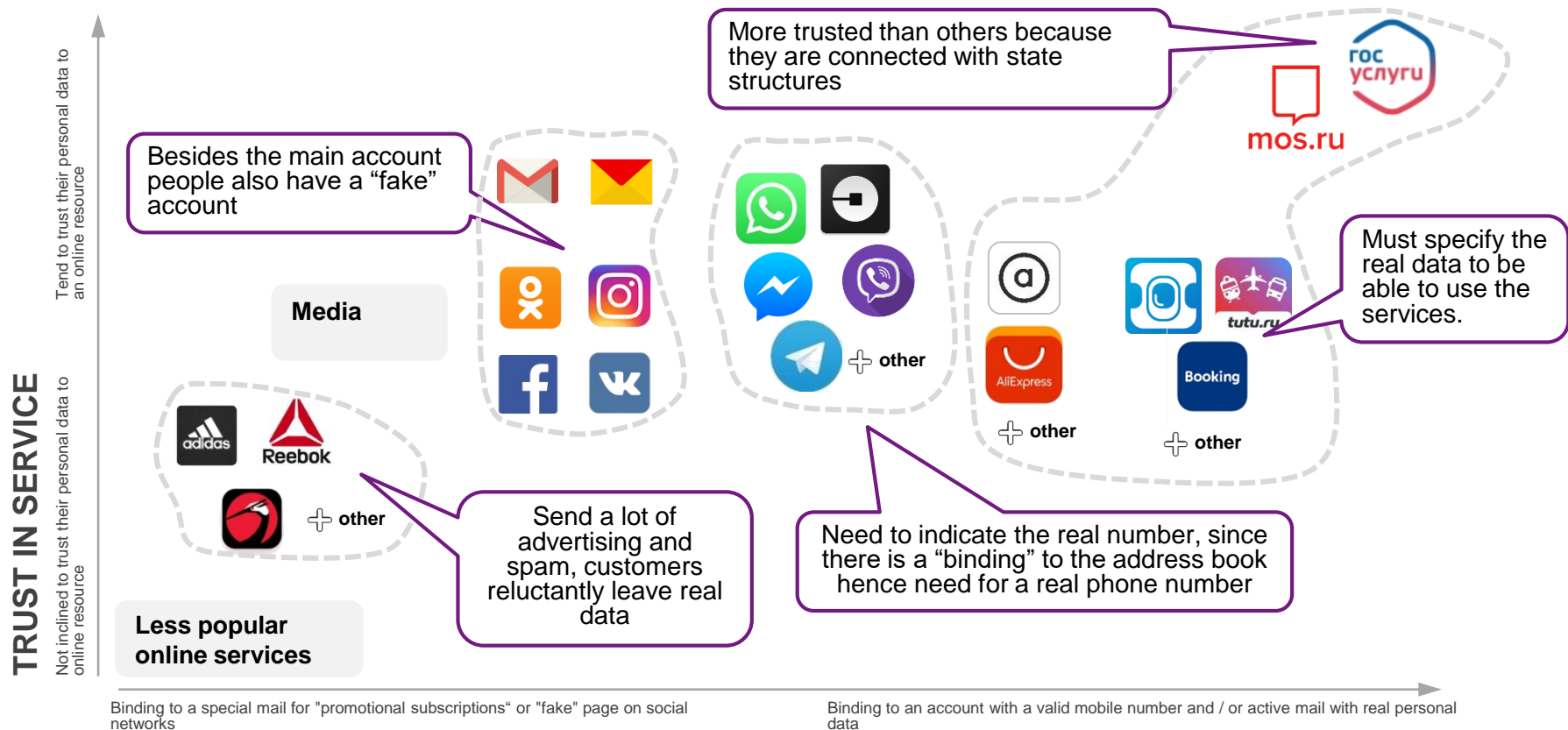
- Study the character of online accounts usage (login / password)
- Determine the relationship to the authentication service using mobile phone and 2 additional functions



Target audience

- MegaFon, MTS, VimpelCom and Tele2 subscribers using online-resources
- Aged 16 – 45

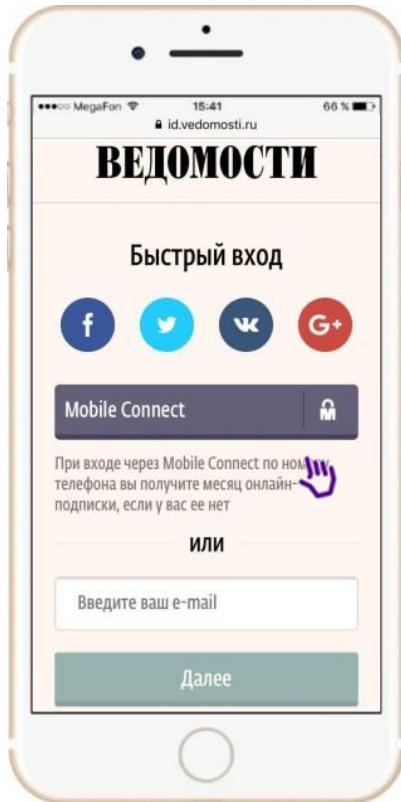
ONLINE RESOURCES USAGE CHARACTER



PROVIDED PERSONAL DATA VALIDITY

RELATIONS TO PRIVACY

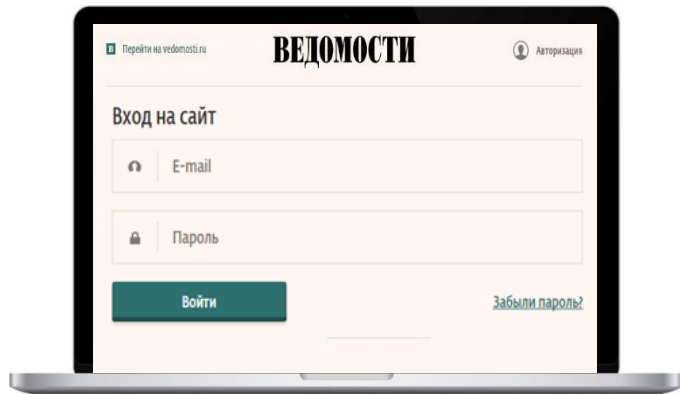
- Users **know about the transfer of personal data** at the login via the social networks and treat this **rather negatively**
- **Differentiate the websites** on which you can or can not use the **login via social networks**
- **Try NOT to use** at the login through the social network **accounts with valid information**
Use those where there is a minimum of information or it is closed or even irrelevant



SIMPLE AUTHENTICATION

SIMPLE AUTHENTICATION

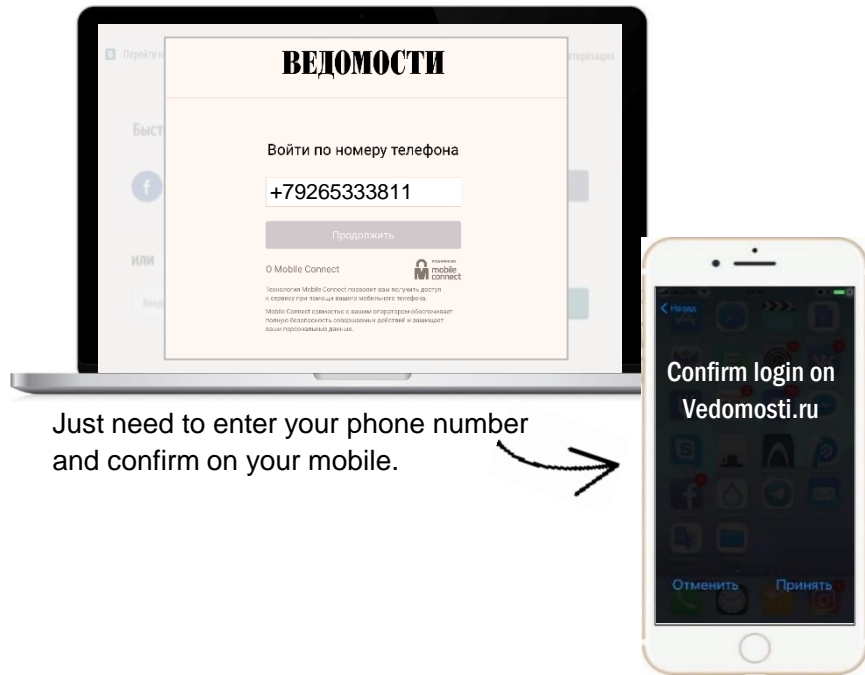
AS IS



Need to create and remember the login and password to register / access the website.



TO BE



Just need to enter your phone number and confirm on your mobile.

SIMPLE AUTHENTICATION: OVERALL IMPRESSION



Interest and attraction

- In general, all age categories liked the service

Convenience and time saving

- No need to remember your password, everyone knows their number by heart
- Mobile phone is always with you
- Minimum steps
- No need to wait for an email, follow links, fill in additional fields



Possible "technical" problems

- Expect recovery problems when changing phone number

Doubts about guaranteed security of personal data

- Website will send spam / advertising
- Operator will transfer personal data to the website without consent.
- Somebody can steal phone and user data



2-FACTOR AUTHENTICATION

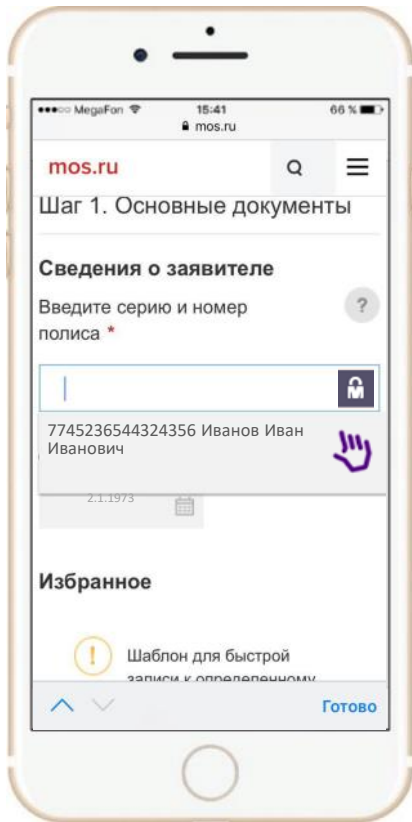
2-FACTOR AUTHENTICATION: OVERALL IMPRESSION



- User does not depend on delayed SMS
- No need to switch between screens to enter a code from SMS
- Single stable PIN
- Secure confirmation of transactions by Touch ID is possible



- Doubts about the security of the service, especially in case of loss or theft of the phone
- Difficulty in changing the PIN when changing the phone number or operator



FORM FILLING

FORM FILLING: OVERALL IMPRESSION



- Save time (and nerves)
- Avoid errors when entering information
- The user decides to whom and what information to provide



- Solves the rare need
- Doubts about the security of the service as a whole
- Failures on websites and, as a result, incorrect filling of fields

2

B2B

QUALITATIVE RESEARCH



MOBILE CONNECT FEATURES STUDY



Objective

- Rate demand and perception of services based on Mobile Connect technology in the target market



Target audience

- Key people in the company who understand how operations of the company is organized for its successful functioning
- Companies with websites asking for:
 - registration to purchase or use the service;
 - personal data to provision the service

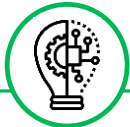


Company size

- 50 to 250
- Over 250

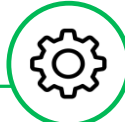
MOBILE CONNECT PERCEPTION

The service is not equally perceived by the interviewed companies



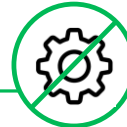
Innovative financially sustainable companies

- Do have money
- Actively use e-commerce
- They know their target audience - they are actively engaged in marketing and research
- Technologies are in priority, ready to invest more.
- Interested in the service



Medium innovative financially unstable companies

- Rather there is no money, often the business is credited
- Often use e-commerce
- They know target audience at the level of intuition. Don't carry out researches - do not see value / there is no budget
- There is a desire and understanding of the value of innovation, but often there are no resources for it.



Conservative financially weak companies

- No money
- Single use cases of e-commerce
- They do not study and poorly understand their target audience and how to work with it
- Not ready for any innovations - they don't understand the value or are generally not aware of this opportunity.

COMMON DRIVERS AND BARRIERS FOR THE TECHNOLOGY



Drivers

The service is perceived at the level of image, not everyone sees a specific product benefit.

- Allows to maintain the image of an innovative technology company that introduces advanced technologies in business processes

- Image of a client-oriented company - customer care, value of its time, attention to the ease of web services usage

- Optimization of business processes, increasing the speed of order processing, revenue growth



Barriers

The service requires resources, but there is no certainty that it will ultimately bring profit

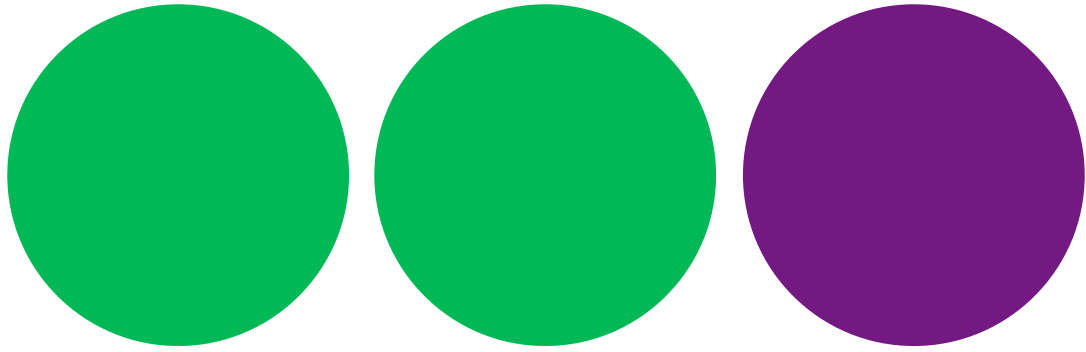
- Uncertainty about efficiency and benefits – whether it will attract new customers, whether the conversion will increase

- The need for additional costs to restructure existing business processes, which is most relevant for financially unstable and developing business

- Conservatism - innovative services can frighten off technically illiterate / non-advanced customers

SERVICE EVALUATION AND TRUST

- **Part of the target audience likes the service, but its usefulness for business raises questions.** Increasing conversion is possible, but not necessary. Requires verification for each specific business.
- Replacing two-factor authentication is also perceived positively, but security raises many questions. **The technology seems attractive, first of all, for banks.**
- **The usefulness of the form filling function is most understandable for business and causes the most positive response**, but only for a business where it is relevant. Ensuring the safety of data use and storage is seen by business as a mandatory function of MC and operators.

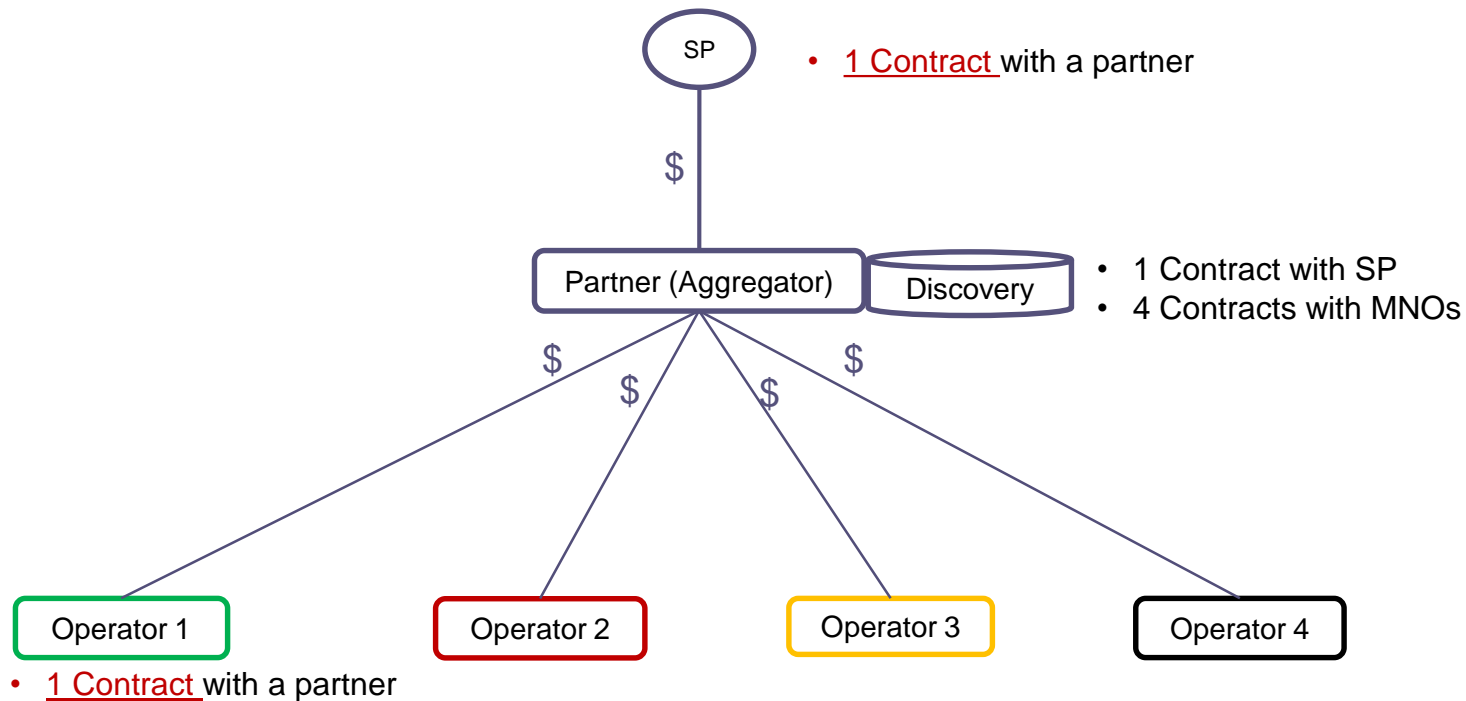


Thank you!

Operators' plans for Mobile Connect introduction in Russia

Ilya Nestor, MTS

Target commercial model for Russia



Product sets considered for introduction in Russia

Basic set

Basic authentication (without PIN)

Secure authentication (with PIN)

Authentication with MSISDN sharing

Authorization (without PIN)

Authorization (with PIN)

Extended set

Network attributes

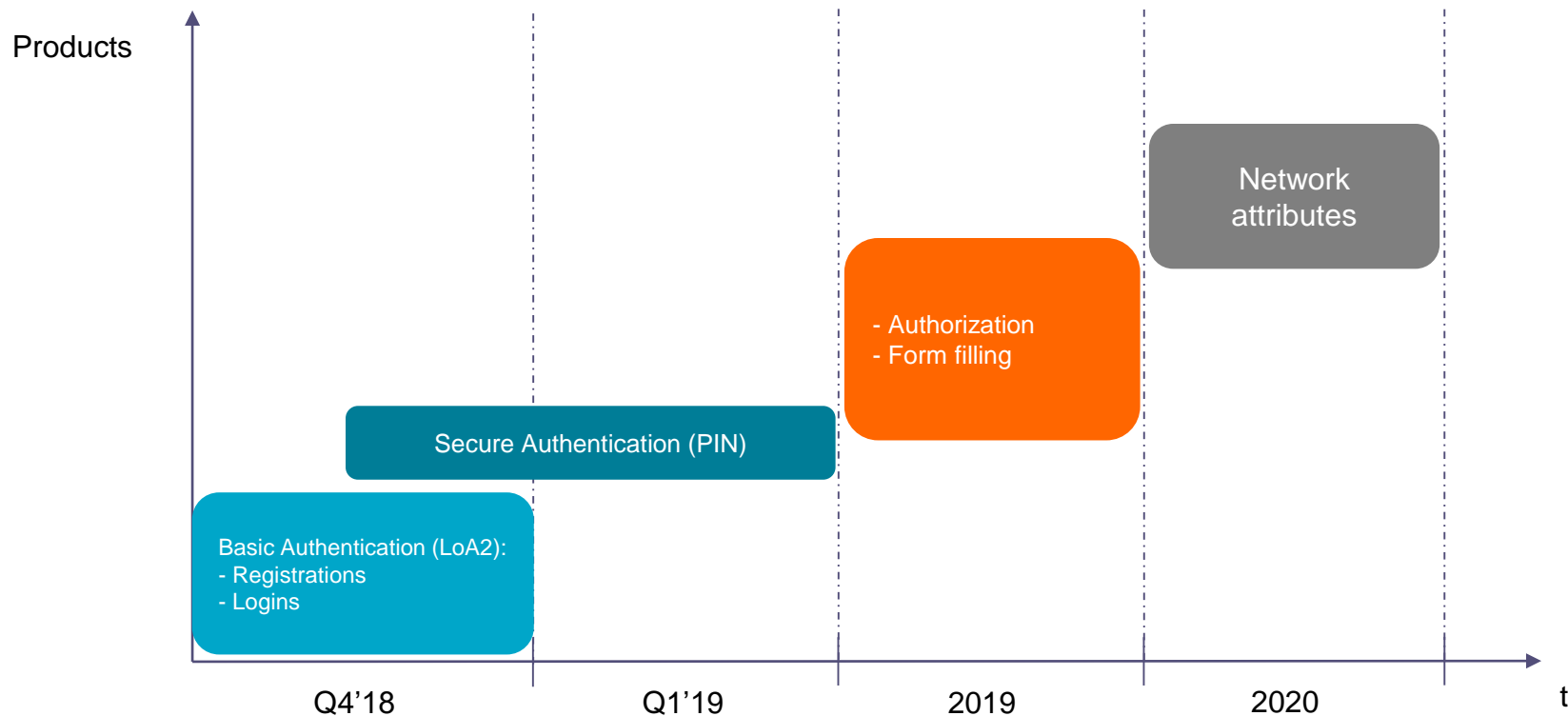
Verification of network data (SIM swap, IMEI network status, geo status)

User's Data

- Authentication (LoA3) with sharing user's data
- User's data verification

- **Targeted advertising** by Operator using Mobile ID (PCR)

Operators' readiness timelines

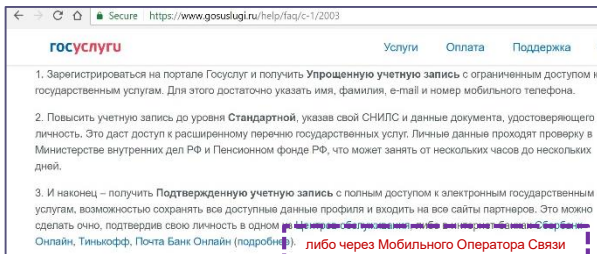


Use Cases for Mobile Connect at Gov portal

Proposal for integration of Mobile Connect service with Gov portal systems to increase the coverage of the census process at the expense of the subscriber base of mobile operators, with the following scenarios:

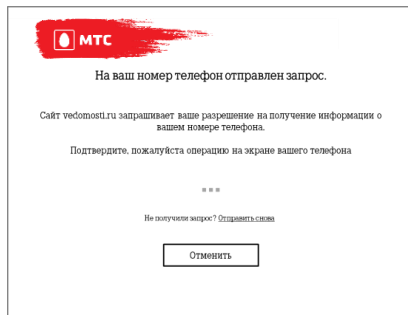
- Gov portal account identification via Operator's self-service
- Authentication on Gov portal with Mobile Connect

Gov portal account identification via Operator's self-service

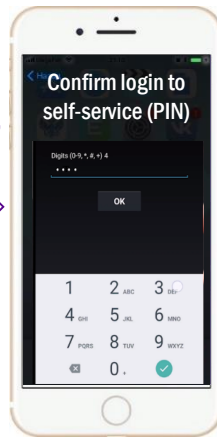


Discovery API

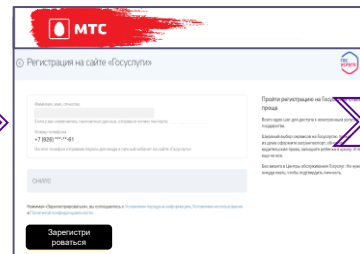
Discovery



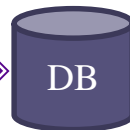
LoA3
(SIM
Applet,
USSD)



OIDC
MC



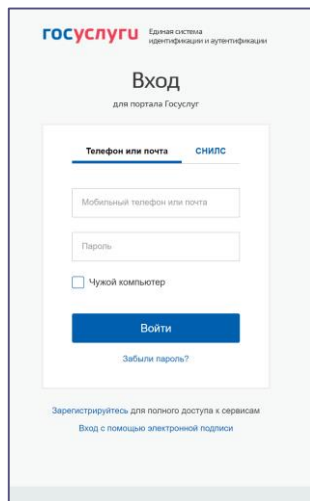
OAuth 2.0



Gov portal

Operator

Proposed use case for authentication on Gov portal with LoA3 [or digital signature]



госуслуги Единая система идентификации и аутентификации

Вход
для портала Госуслуг

Телефон или почта СНИЛС

Мобильный телефон или почта

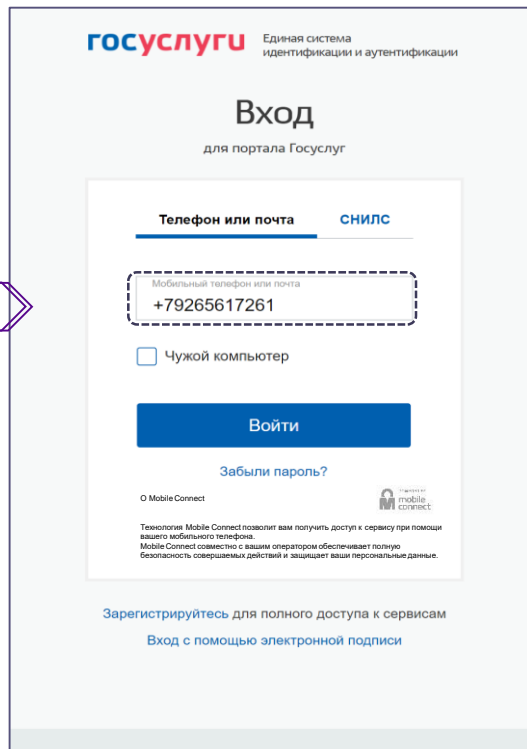
Пароль

☐ Чужой компьютер

Войти

Забыли пароль?

Зарегистрируйтесь для полного доступа к сервисам
Вход с помощью электронной подписи

госуслуги Единая система идентификации и аутентификации

Вход
для портала Госуслуг

Телефон или почта СНИЛС

Мобильный телефон или почта
+79265617261

☐ Чужой компьютер

Войти

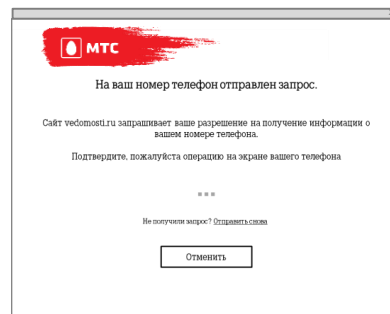
Забыли пароль?

O Mobile Connect

Технология Mobile Connect позволит вам получить доступ к сервису при помощи вашего мобильного телефона.
Mobile Connect совместно с вашим оператором обеспечивает полную безопасность совершаемых действий и защищает ваши персональные данные.

Зарегистрируйтесь для полного доступа к сервисам
Вход с помощью электронной подписи

OIDC
MC

МТС

На ваш номер телефон отправлен запрос.

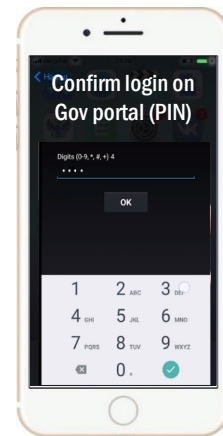
Сайт gosuslugi.ru запрашивает ваше разрешение на получение информации о вашем номере телефона.

Подтвердите, пожалуйста операцию на экране вашего телефона

Не получили запрос? Отправить ссылку

Отменить

LoA3
(SIM
Applet,
USSD)

Confirm login on
Gov portal (PIN)

Digits (0-9, *, #, +) 4

OK

1 2 abc 3 DEF

4 GHI 5 JKL 6 MNO

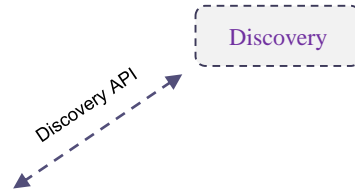
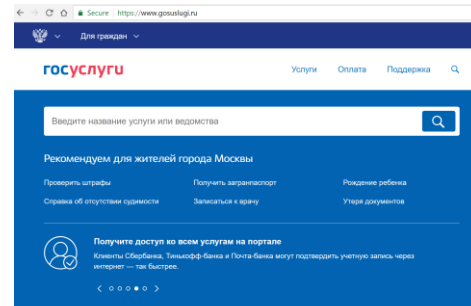
7 PQRS 8 TUV 9 WXYZ

0 +

OIDC
MC



Operator





**MOBILE
360
SERIES**

RUSSIA & CIS
MOSCOW • 30-31 OCT 2018

International experience of using the Mobile Connect solution for government services

- Orange France experience with Mobile Connect et moi – Serge Llorente, (Orange France)
- European eIDAS integration with Mobile Connect– Laszlo Toth (GSMA)



RUSSIA & CIS
MOSCOW • 30-31 OCT 2018

France Connect + Mobile Connect et Moi. A Stake for digital identity

**Serge Llorente
Orange/Mobile Connect Director**



Evolving trends in digital identity. Mobile Connect and the eIDAS cross-border pilot

Laszlo Toth - Head of Public Policy – Europe, Russia & CIS

31 October 2018

The importance of digital identity



Advanced technologies that deliver **robust, secure** and accessible authentication services to all



Empowers citizens to take control of their privacy, **strengthens security**, and **builds trust**



Opportunity for governments to provide access to key services utilising the **security of operator networks**



883 million

SIM connections in Europe, by 2020*

€674bn (3.9%)

Mobile industry contribution to GDP in Europe, by 2020*

Mobile authentication:

An evolving market place



Growing awareness of privacy and data protection is **driving demand**



Cyber crime is driving up the value of **secure identity verification** with users' attributes



Operators are well positioned to work with **governments** to deliver attractive identity services

Mobile Connect

Over 70 operators in nearly 40 markets



Mobile ID on public services show extraordinary adoption rates



EU 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).

eIDAS and Mobile Connect cross-border pilot



Mobile Connect for
Cross-Border Digital Services
Lessons Learned from the eIDAS Pilot

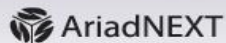


Building trust in the online world is crucial to accomplish the Digital Single Market. Coupling mobile authentication credentials, such as Mobile Connect, with the identity security provided by eIDs under the eIDAS Regulation, is the way towards this goal



Andrus Ansip
Vice-President of the European
Commission for Digital Single Market

#eIDAS
@eID_EU



CLAYSTER



Difi

Agency for Public Management
and eGovernment



E-LEGITIMATIONS
NÅMNDEN



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY



WITH THE SUPPORT OF THE EUROPEAN COMMISSION

Pilot scope

- **Regulatory interoperability:**
 - Mobile Connect authentication and validation of the citizen's digital identity across France, Norway and Sweden using their eIDAS Nodes
- **Technical interoperability:**
 - Developed and tested the eIDAS Reference Architecture and demonstrated interoperability of Mobile Connect with eIDAS nodes integration requirements in a live test environment
- **Owner Centric Model:**
 - Showcased Mobile Connect secure authentication and eIDAS identity to access healthcare private sector services in a Internet of Things application environment

Government initiatives with Mobile Connect



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



EU – eIDAS Phase I European-wide solution for log-in to government services

EU – eIDAS Phase II European-wide solution for public and private online healthcare services



UK – user identity verification service to confirm identity for e-Government services

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



Spain – Use of Mobile Connect to log into digital public services in Catalonia



France – French government with Orange France on accessing government services using Mobile Connect



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

Additional information

- GSMA Identity Programme:
<https://www.gsma.com/identity/>
- Mobile Connect Website:
<https://mobileconnect.io/>
- GSMA eIDAS pilot report:
<https://www.gsma.com/identity/mobile-connect-cross-border-digital-services-lessons-learned-eidas-pilot>



MOBILE
360
SERIES

RUSSIA & CIS

MOSCOW • 30-31 OCT 2018

#M360RCIS