24 March AssureUK
All Hands Meeting



Restricted - Confidential Information

All GSMA meetings are conducted in full compliance with the GSMA's anti-trust compliance policy

Andy Rudd +44 7860 400 950
arudd@gsma.com

Welcome

Todays focus

UK Ecosystem – Daily Transactions: Banking

We'll cover

1. **In market experience - MobileID and BankID (Nordics)** — **Janne**
2. **UK Banking and Mobile linkage** — **Sharon**
3. **"I'm in control", what the end-user wants** — **Colin**

4. **Table breakout**
   a. what shape should AssureUK take for banks and mobile operators?
   b. What are the benefits of a central exchange vs. sector-specific exchange vs. bi-lateral data interchange agreements?
   c. What is the best next step?
5. **Rapid fire feedback** — **All**

6. **AssureUK progress and forward plan** — **Andy**
7. **Networking, cakes and tea** — **Lounge**

We'll cover

1. **In market experience - MobileID and BankID (Nordics) Janne**



Views on Mobile ID in Banking

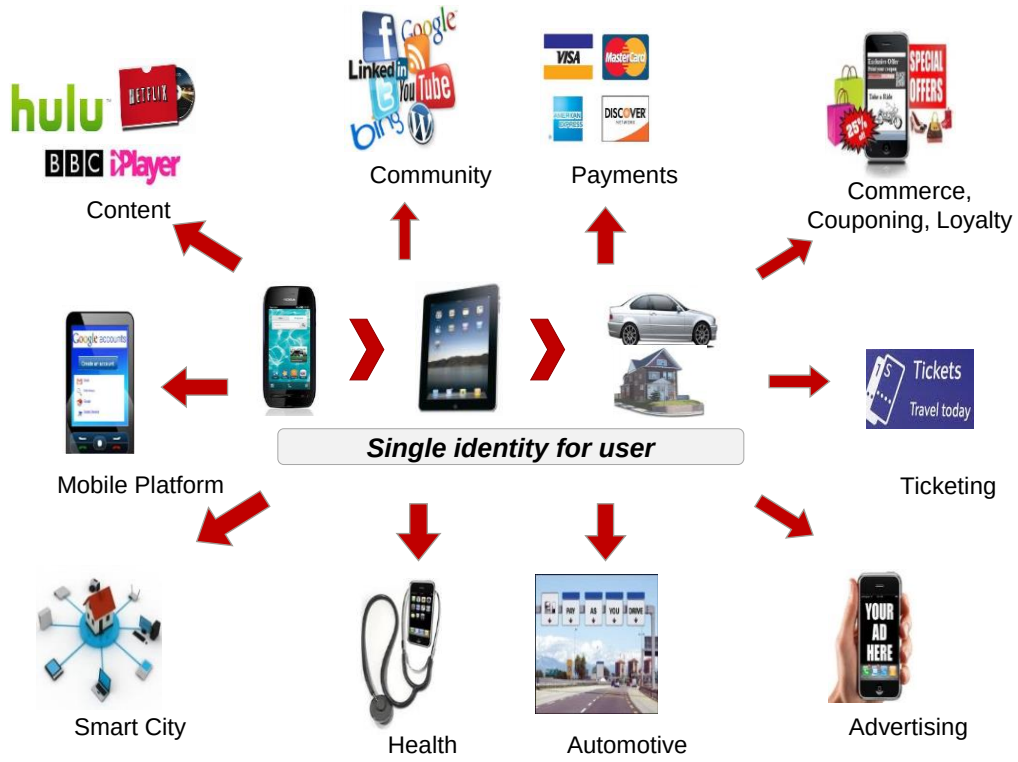
24th March 2014, Janne Jutila, GSMA Personal Data

Re-thinking identity – Moving from industry silos to customer's view of world

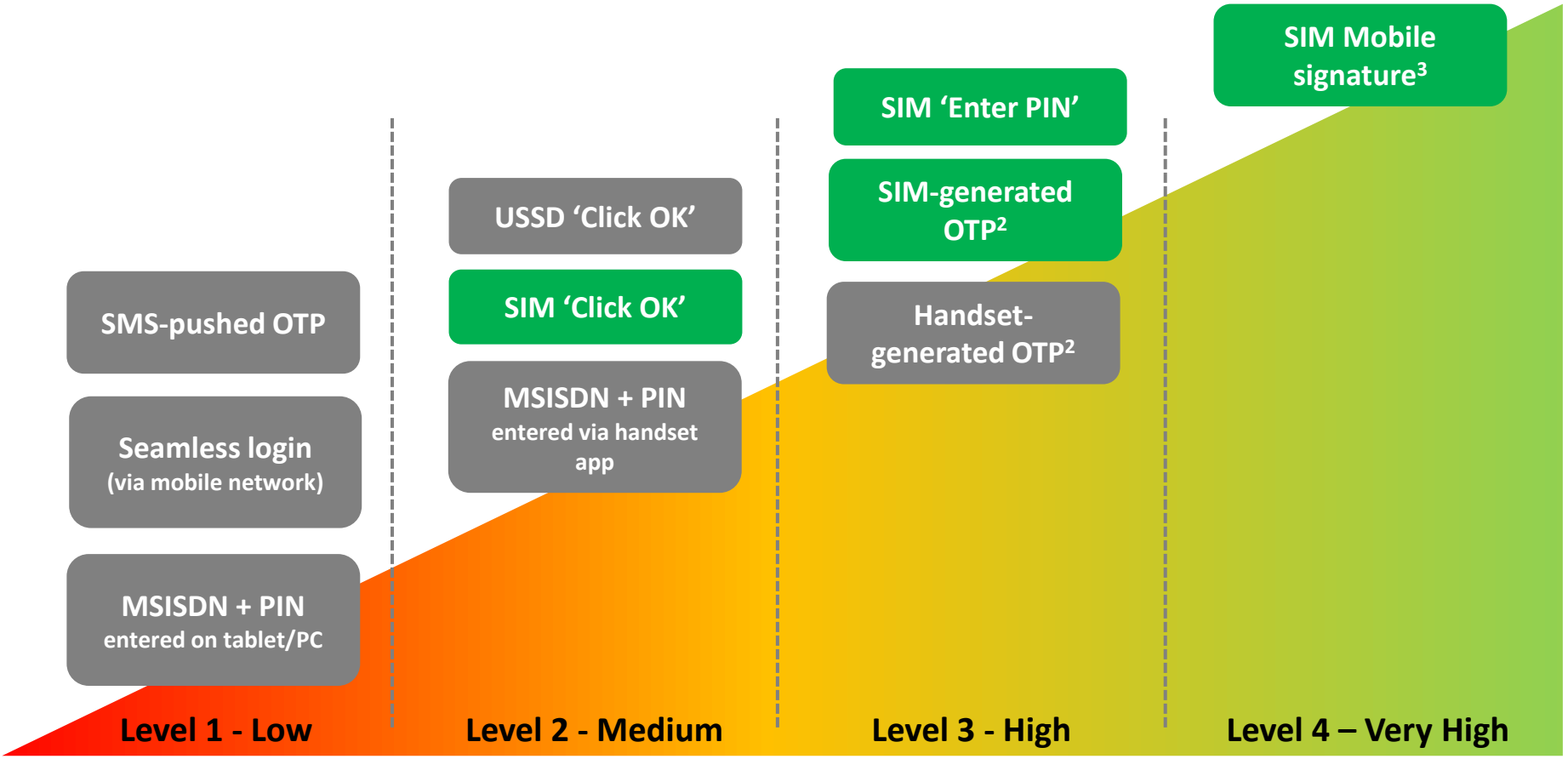
Industries are here!

Banks	OEMs	Online players	Operators
DNB	NOKIA	facebook	telenor
citibank	Motorola	Windows	axiata
HSBC	HTC	Apple	at&t
NatWest	SAMSUNG	Google	vodafone
Deutsche Bank	intel	in	orange
THE NISHINIPPON BANK,LTD.	HUAWEI		kt
Nordea			TIM

How do we get here?



There are many mobile technologies available that deliver authentication at different LOA's[1]



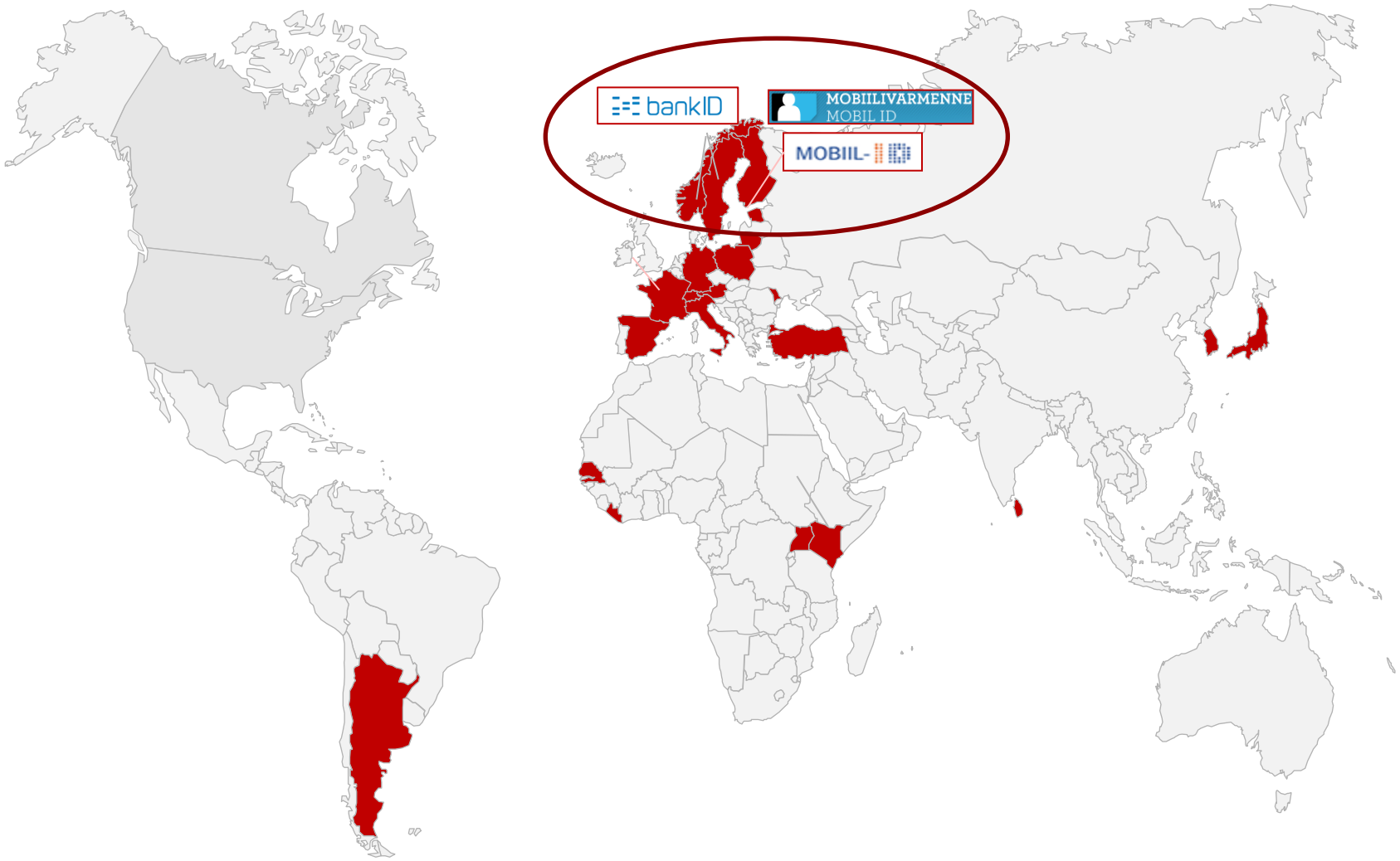
[1] Levels of Assurance based on ISO/IEC 29115 Clause 6
[2] Generation of a One-Time-Password on the SIM or an application running in the handset
[3] SIM PIN + wPKI

Personal Data

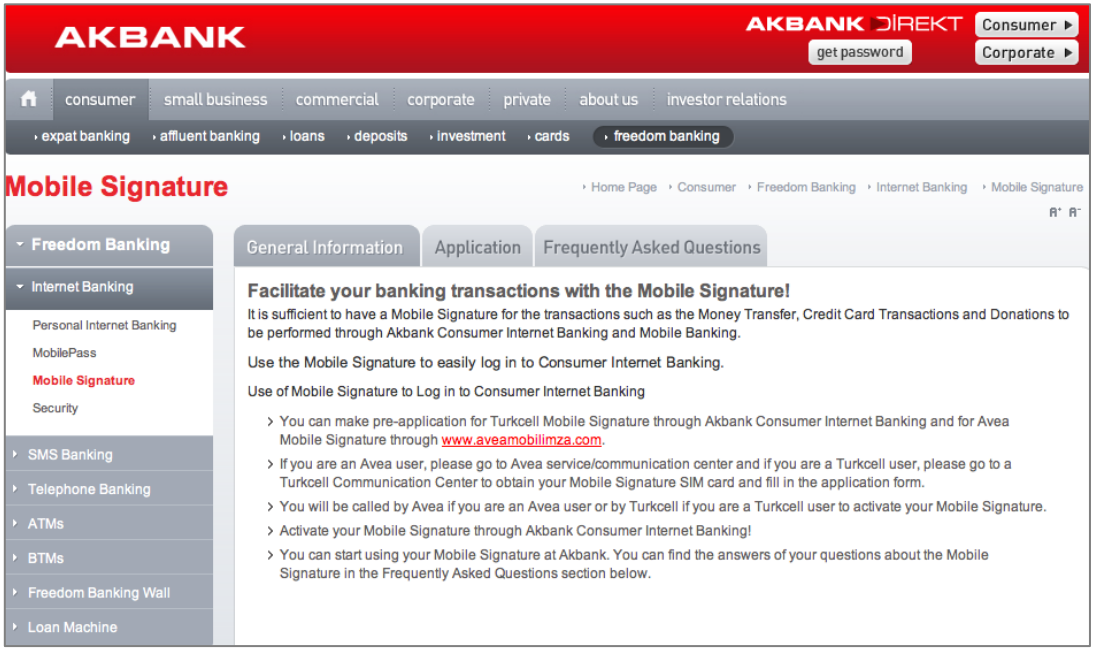
© GSMA 2014

Why are these small Nordic countries interesting in Mobile ID?

-Leaders in online & mobile rankings, well-established ecosystems, different market models



Priority Banking Use Cases – *Online Access*

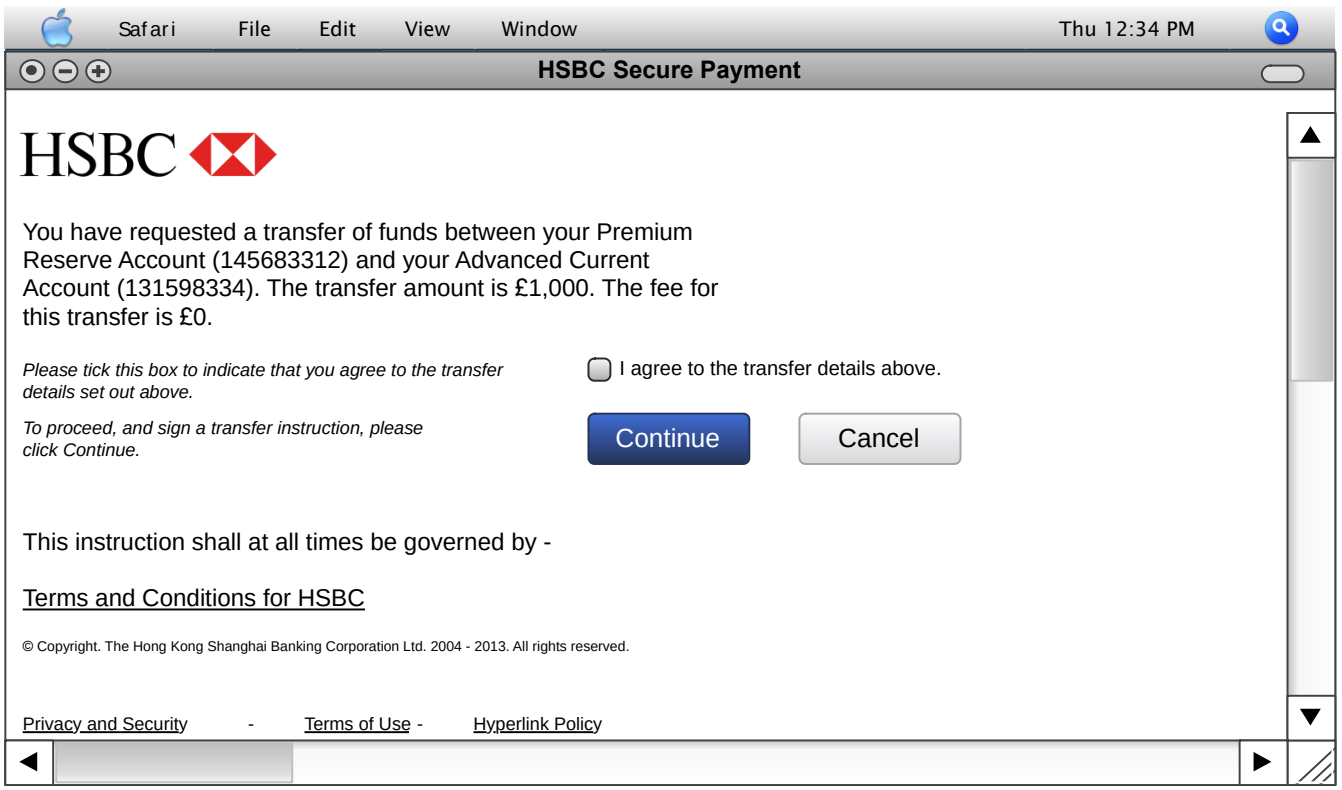




- Increasing the security of online banking is a priority for banks themselves, and for their customers
- The traditional username and password is too weak, and TAN hardware tokens are extremely expensive, difficult to use and easily lost
- Mobile signature services can provide materially higher levels of security, for lower cost, with substantially greater levels of usability
- Services have been successfully deployed against such use cases in Turkey, Finland, Estonia, Norway, Sweden and elsewhere

Source – AK Bank / Turkcell (service live)

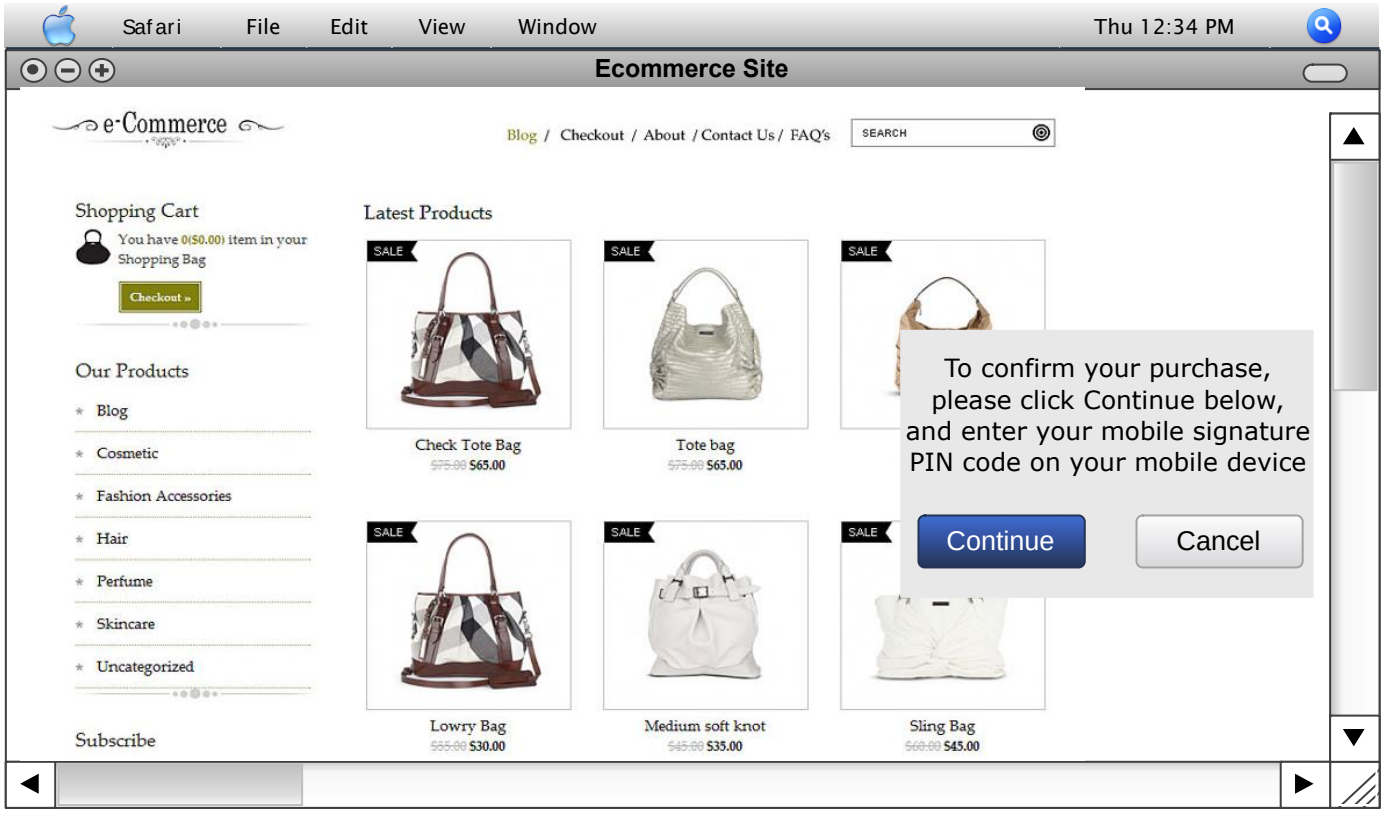
Priority Banking Use Cases – *Transaction Auth*

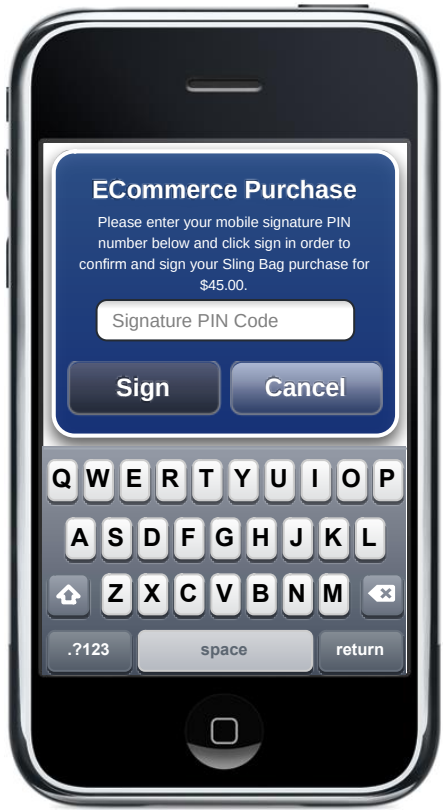




- The use of online banking on a PC, supported by mobile signature on the handset, arguably represents the optimal use case from a security perspective: the authentication presented here is inherently multifactor, and if architected carefully, can be highly resistant to man-in-the-middle and man-in-the-phone attacks; it is also resistant to keystroke loggers and similar, since the login credential is presented via the mobile phone, not the personal computer

Priority Retail Use Cases – *Online Transactions*





- Mobile signature can add substantial security to online commerce – in the majority of cases, ecommerce sites are protected only by username and password credentials, which are weak, and readily stolen or guessed
- Mobile signature adds not only an additional factor, but also serves to reassure both buyer and seller that the transaction has a clear status in law, with clearly articulated rights and obligations known to both parties

Mobile ID in Finland

Electronic ID on the phone SIM card

Common service from leading Finnish operators

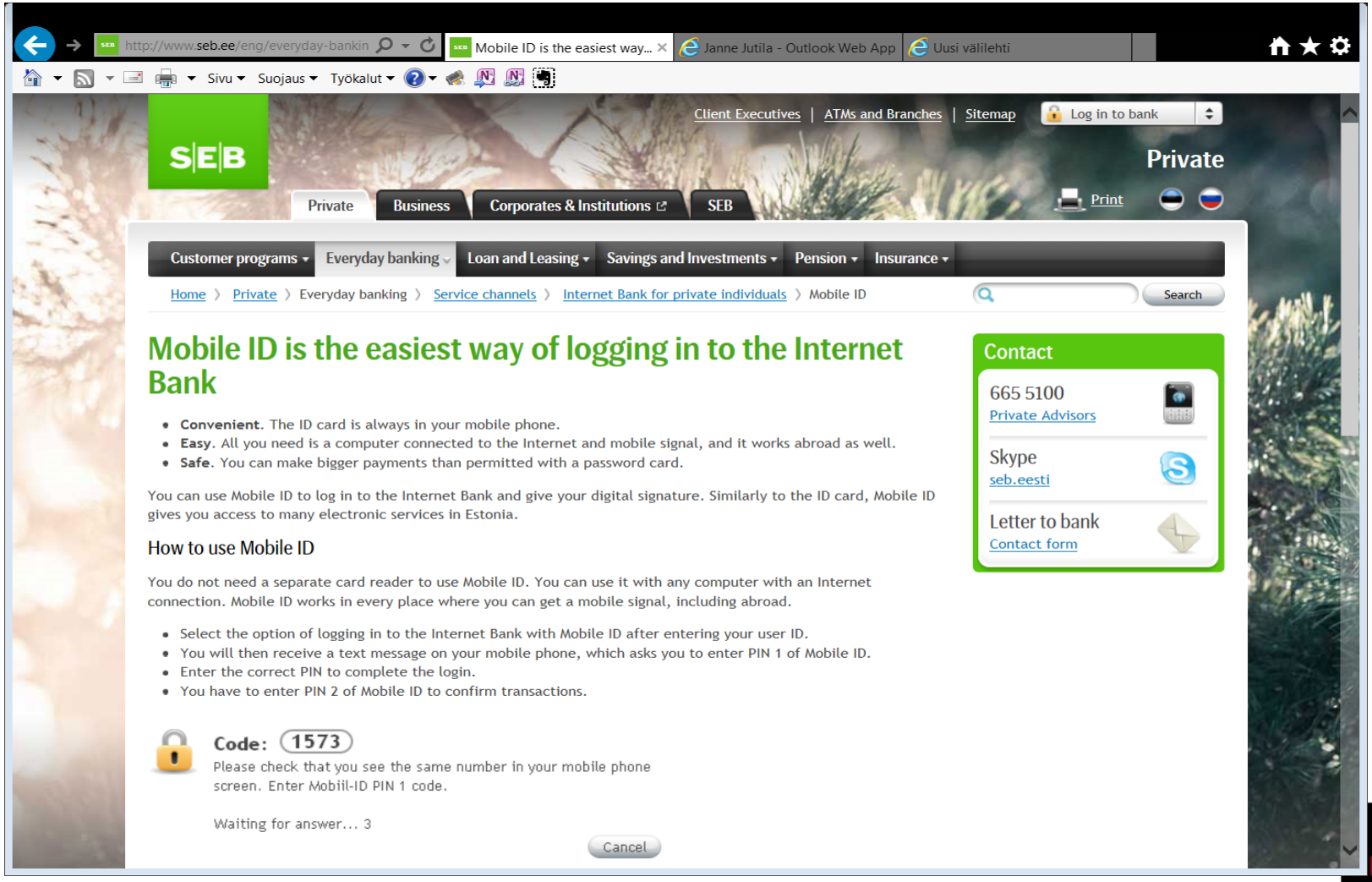
- Strong authentication according to the law
- ”Trust network” between operators
- Single agreement and integration to reach all users
- Mobile ID registration with home operator (operator store, internet with Bank ID)

Mobile ID - tool for convenient and secure eTransactions

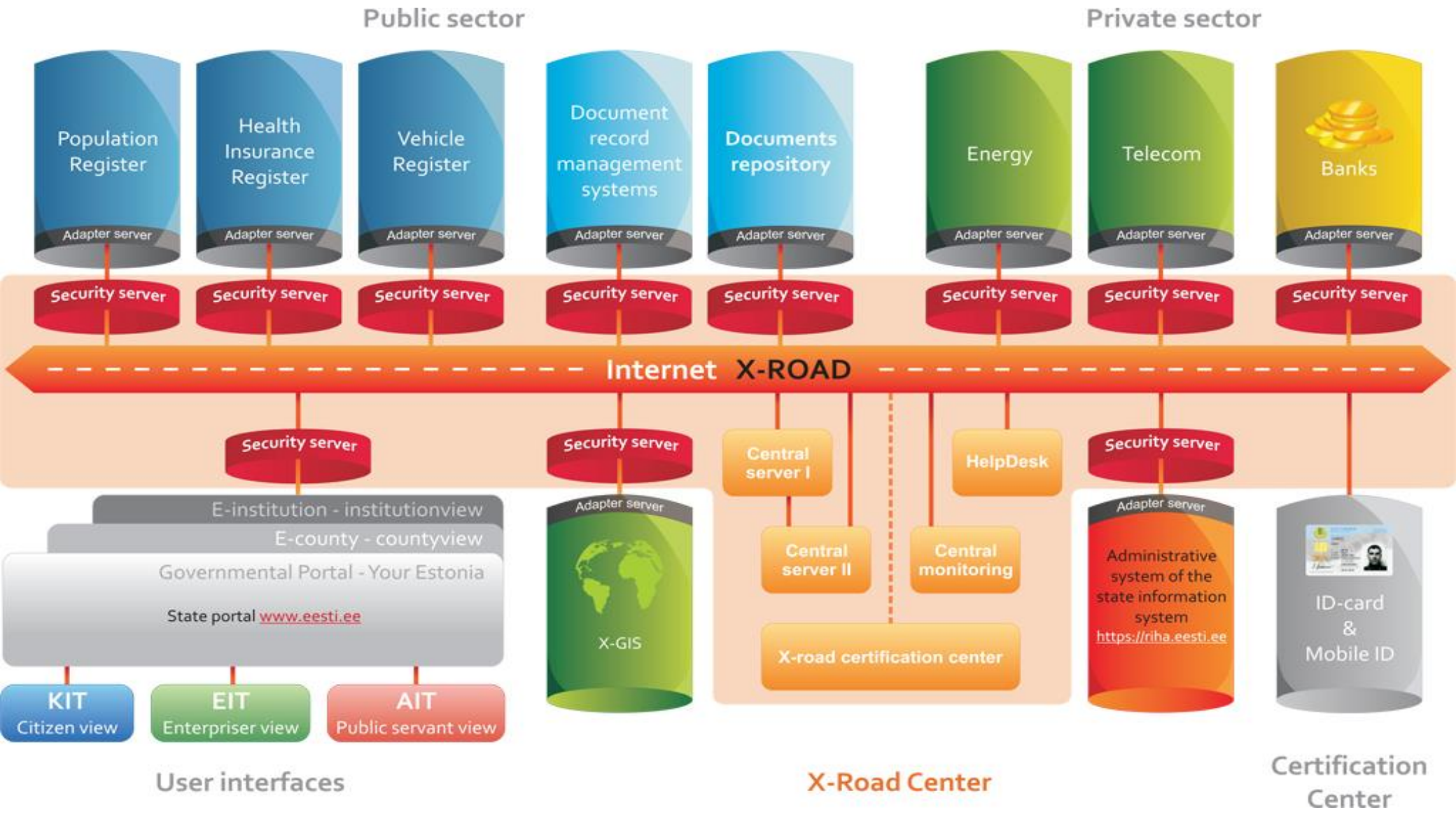
- GSM number + Mobile ID PIN-code
- Same user-experience across all channels and services: web, mobile, phone call
- Clear roles between players
- Simple, transparent business model

Seamless eServices ecosystem from operators – authentication, authorization, payment approval

Banks using Mobile ID as easiest (and safest) way to log-in in to your Internet Bank

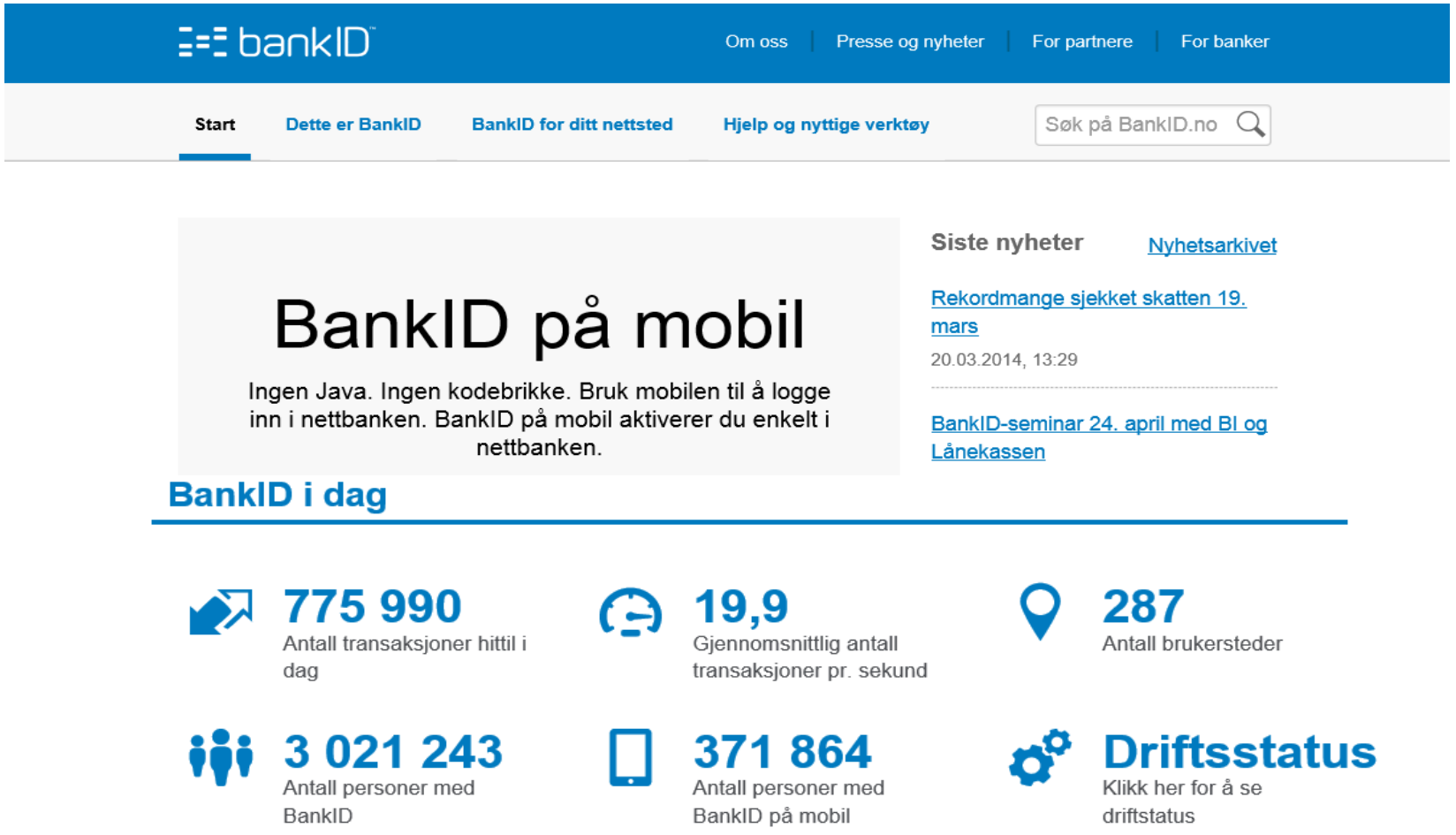


Example Ecosystem - Estonian Information System

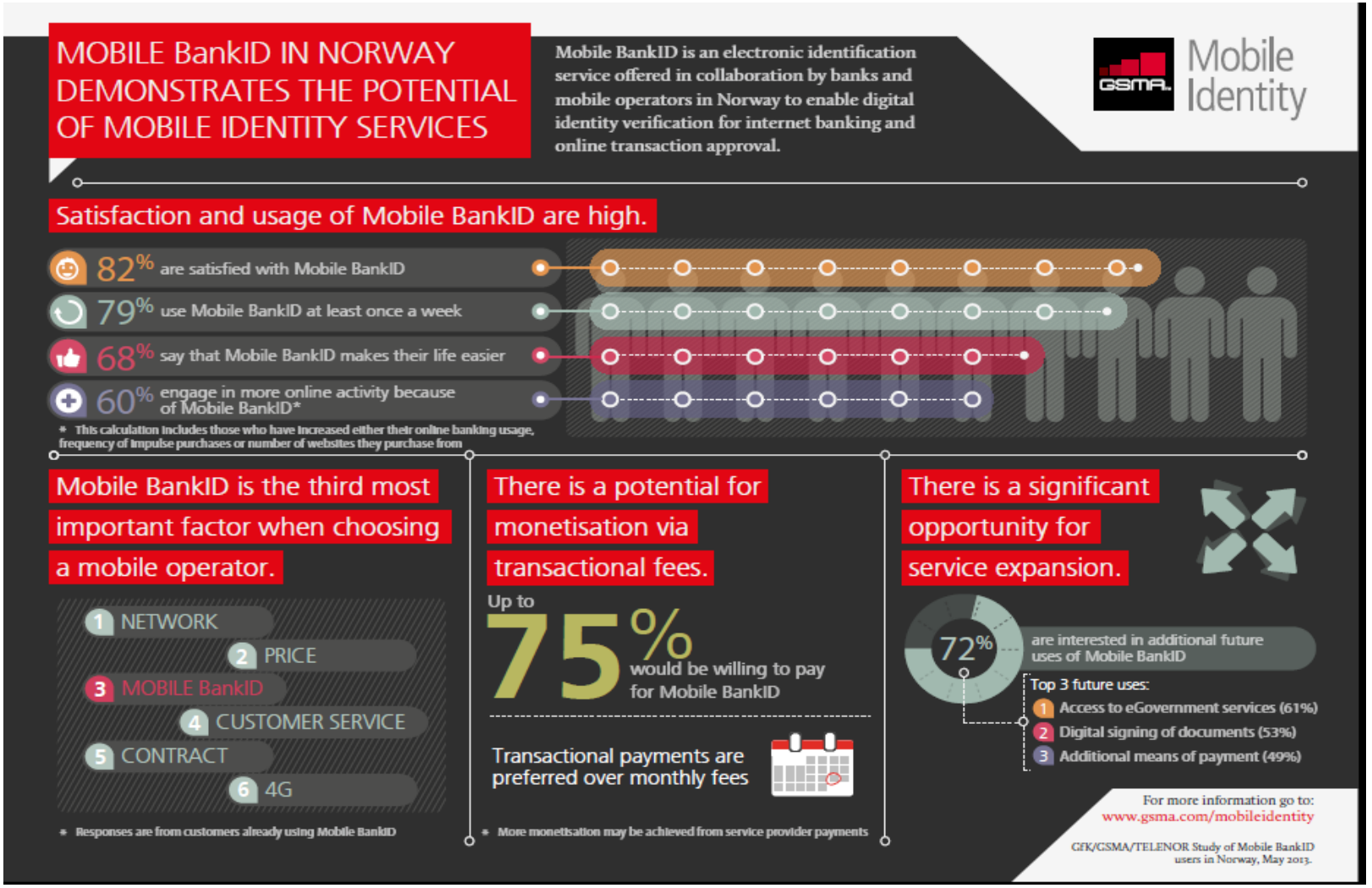


X-Road was launched in 2001

Mobile Bank ID in Norway



Mobile Bank ID in Norway showing great user



There are minor user issues with the Mobile BankID usability, but none grave enough to stop usage

Speed

Only 60% in quant satisfied with speed

Small delay between authorisation and screen change

'It's slow. I use Scandiabank and there it's still quicker to choose your password on SMS so I swap between the two.'

Crashes

authorisation process stops occasionally and has to be restarted

'I have had quite a few crashes with it, with mobile and that service, it's clumsy, if you put the wrong code in 3 times it closes it down.'

79% in quant feel the service always does what they want

Tedious processes

'To pay bills you do it once, then do it again, put code in twice, that's a bit irritating. You shouldn't have to sign again, you have to sign a number of times.'





Problems using the service abroad

minority have experienced minor problems especially US

'It wouldn't work so I had to restart the service when I got back to Norway'.'

Different layouts

no uniform Mobile BankID design across different websites

77% in quant feel the service is consistent across websites

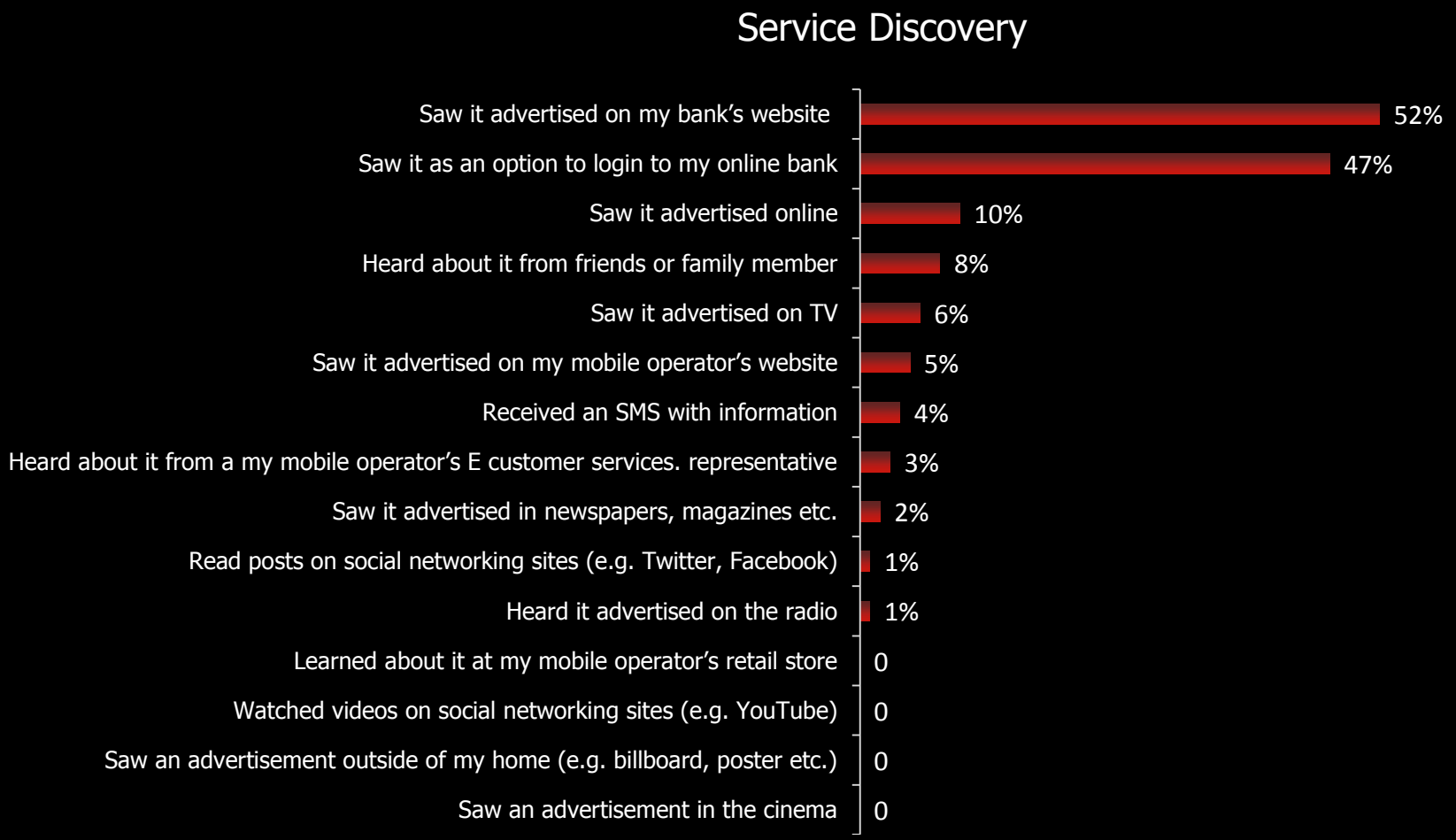
Entering a wrong code

without realising they are inputting

Screen lock

interrupting authentication process

Majority discovered service when logging onto their online banking



Source: Mobile BankID Norway Study
Base: All Respondents (903)

Four reasons why MNO's and banks are natural partners in Mobile ID

Secure ID registration and fast scaling to whole customer base[1]

Pre-populating NFC/ID SIM's

Service discovery as part of online banking experience

ID proofing with existing ID's and/or physically

Multi-channel customer service & local support for all consumption devices







Unparalled convenience combined with high security and user control

Trustworthy & locally regulated



1) User = ID subscriber = customer; SP = Service Provider = Relying party = "merchant"



Thank you

Janne Jutila, GSMA Personal Data

We'll cover

1. In market experience - MobileID and BankID (Nordics) Janne
2. **UK Banking and Mobile linkage** **Sharon**

The existing LINK between MNOs & Banks

Sharon Hetherington

VOCALINK
safer payments, smarter partner

Why am I here?

Overview of VocaLink's position in the UK's financial services market and our link to the UK's Mobile Network Operators

How we are currently evolving this capability

To promote thinking of how this technical asset can be re-used

Market Forces

Consumer demand for convenience – fast, simple, anywhere, anytime…. Plus secure, and private



Consumer



Technology

Technology enabling change:
- Smartphones
- Virtual Wallets

Payment Channels

Banking Community



- Banks adding new functionality
- Valuable KYC capabilities
- Maintaining control of payments

Market changes generating new payment options for Service Providers

Vendors



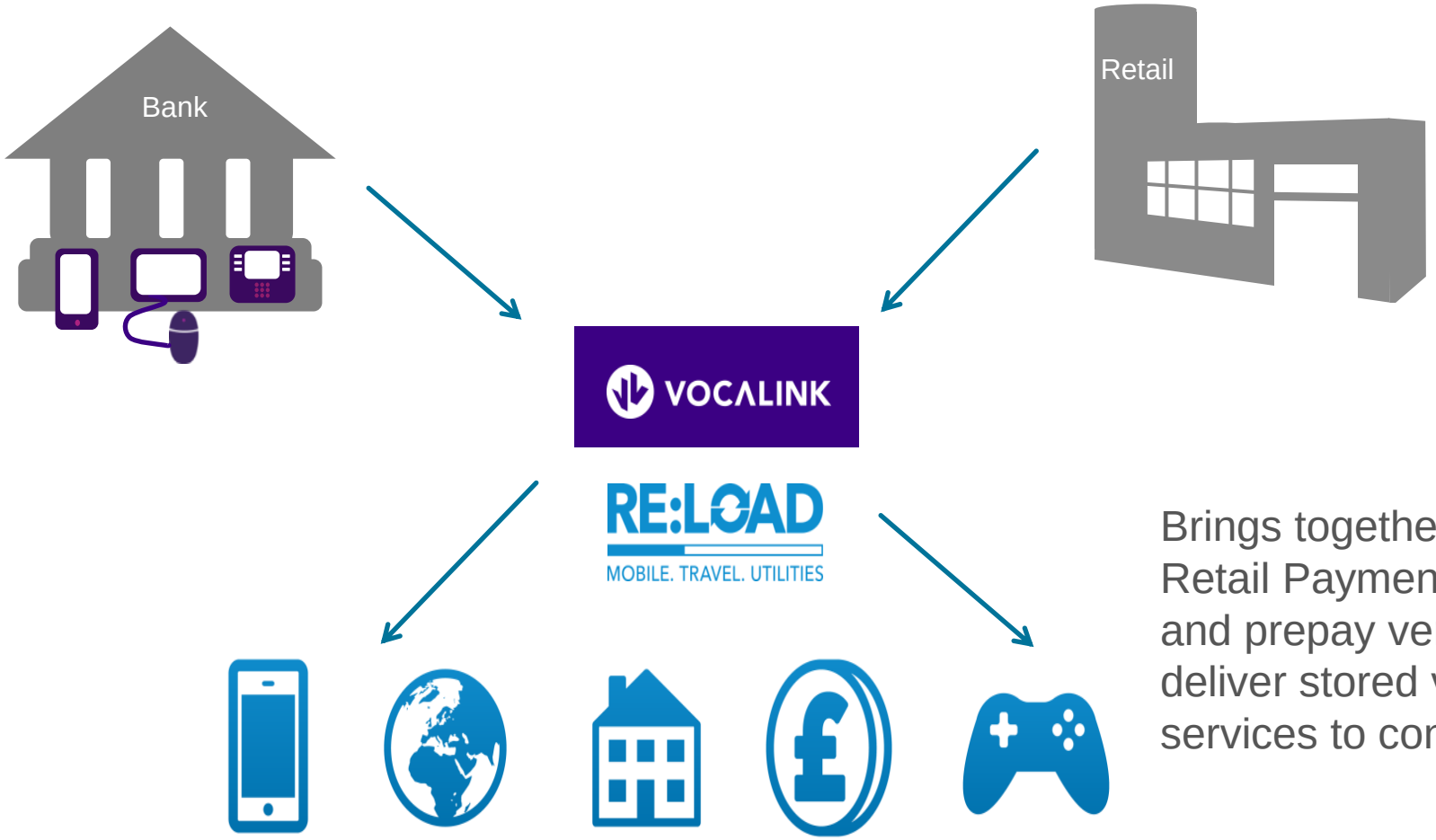
VOCALINK
safer payments, smarter partner

Existing Secure & Trusted Connections



VOCALINK
safer payments, smarter partner

Re:Load



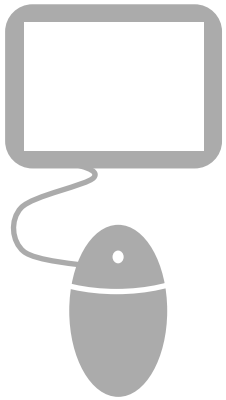
Brings together Banks, Retail Payment Networks and prepay vendors to deliver stored value reload services to consumers

VOCALINK
safer payments, smarter partner

Supporting prepay markets for over 12 years…



Mobile banking



Internet banking



ATM

VocaLink Re:Load Service

10 Mobile Network Operators

1 Mobile Banking App Provider

17 UK Banks

VOCALINK
safer payments, smarter partner

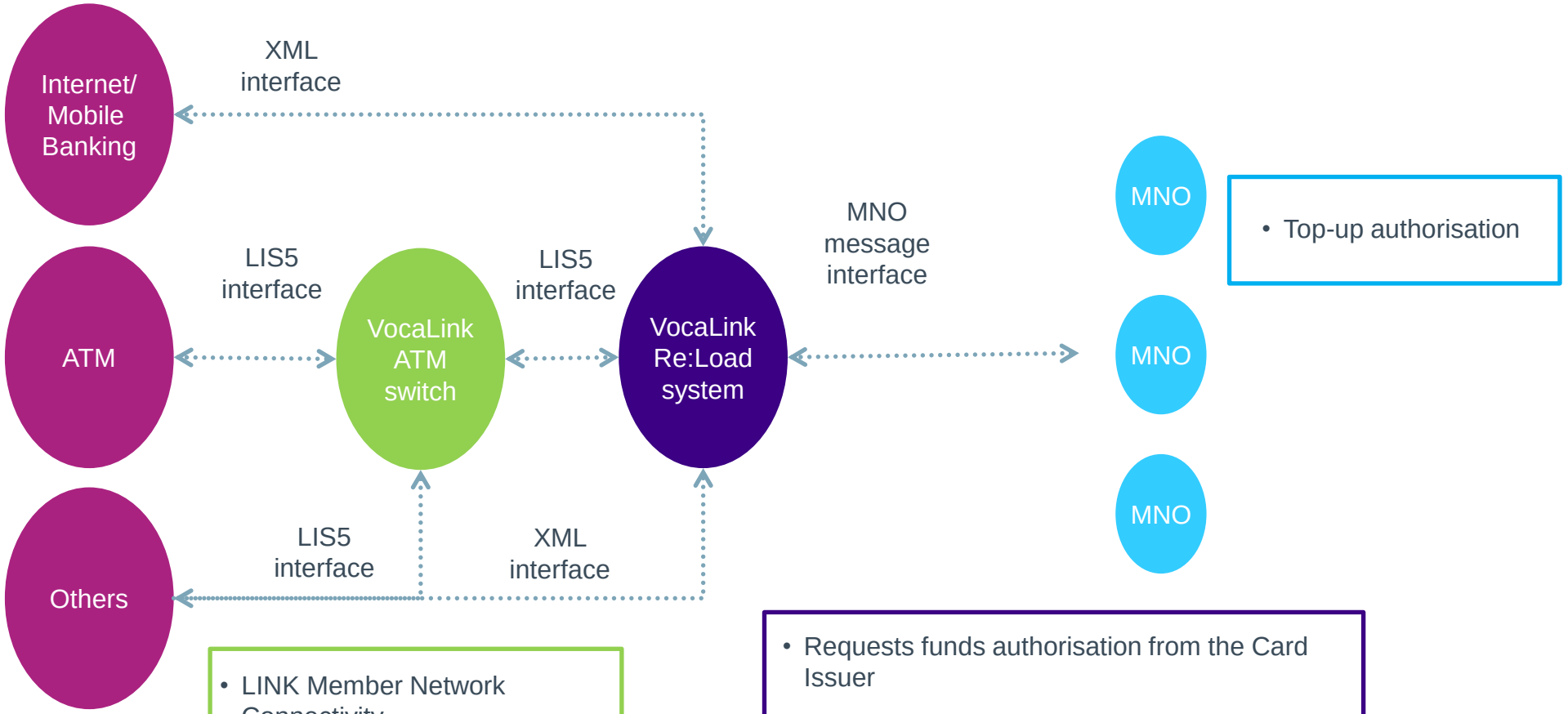
Evolved from the ATM Service

- Launched in 2002
- Bank card + PIN + MNO + mobile number
- Real-time funds authorisation – pay first mechanism
- 80% ATMs UK offer airtime Top-up
- 90% Cards UK support airtime Top-Up
- Processing 8 million transaction per annum, value of £96 million



Mobile phone
airtime top-up demo

Solution Overview



- Top-up authorisation

- LINK Member Network Connectivity
- Transaction switch
- Controls settlement/payment

- Requests funds authorisation from the Card Issuer
- Requests top-up from MNO
- Calculates fees due from the MNO

VOCALINK
safer payments, smarter partner

Assets



Connectivity to 31 UK's Banks

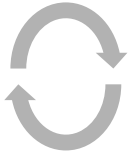


Connectivity to 2 Retailer Payment Networks – Paypoint and Post Office



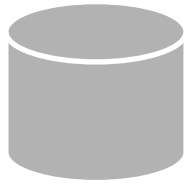
Connectivity to 10 Mobile Network Operators

Secure transaction switching and payment processing



ATM, Retail, Internet and Mobile Banking Channels





Processing data LINK, Faster Payments, BACS and Mobile P2P Proxy Database

Single point of convergence
Interoperable assets
Extendable message standard

VOCALINK
safer payments, smarter partner



VOCALINK

safer payments, smarter partner

We'll cover

1. In market experience - MobileID and BankID (Nordics) — Janne
2. UK Banking and Mobile linkage — Sharon
3. **"I'm in control", what the end-user wants** — **Colin**


GfK
THE CONSUMER PERSPECTIVE
@COLINSTRONG

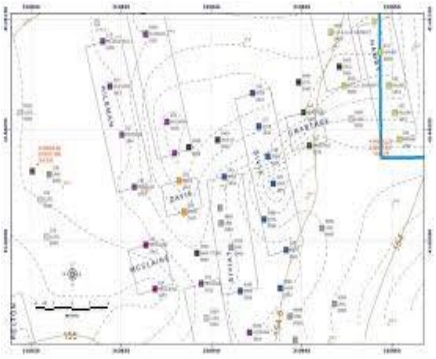
Big Data can tell us a lot about ourselves:

Disciplines are revolutionized by the development of novel tools: the telescope for astronomers, the microscope for biologists, the particle accelerator for physicists, and brain imaging for cognitive psychologists. [Big Data is] a high-powered lens into the details of human behavior and social interaction that may prove to be equally transformative.

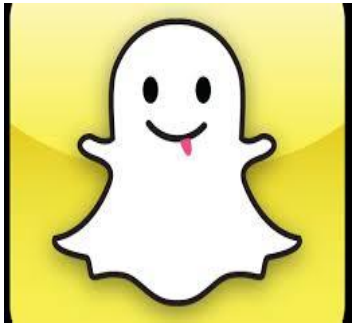
Scott Golder







We are seeing a sharp rise in consumer interest and take-up of privacy related products and services:







ShazzleMail







And there is huge, adverse consumer reaction to perceived breaches of privacy





care.data



We are seeing the way in which personal data is used becoming a source of differentiation for brands:

69%

Find it creepy the way that some companies use information about me

GfK 2013

90%

Prefer to do business with companies that respect my privacy

GfK 2014





On-line advertising, the fundamental business model for the Internet is facing problems:

39% +30%

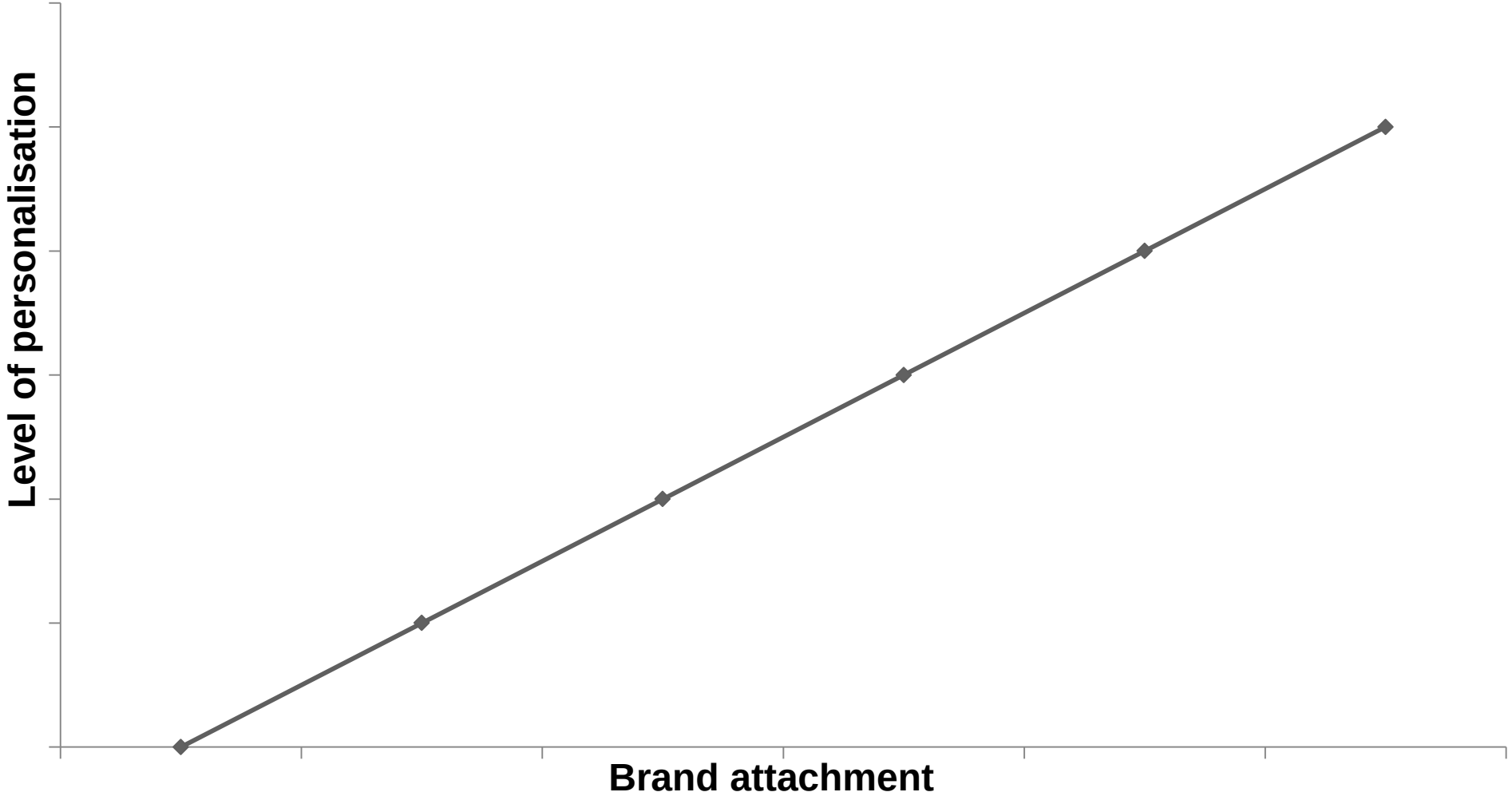
Take steps to block online advertising

GfK 2014

Would block online advertising if it was easy to do so

GfK 2014

Implicit assumption of a linear relationship between personalisation & brand attachment:



But our relationship with technology is a complex one:

- Recent study found that humans would follow a robot's orders to perform tasks even when they did not want to
- Under human authority 86% of subjects begrudgingly finished their arduous file naming task
- Under robot authority 46% of subjects finished their tasks – lower but still a significant proportion
- Reminiscent of Milgram obedience tests



And the ‘Uncanny Valley’ suggests a complicated relationship:

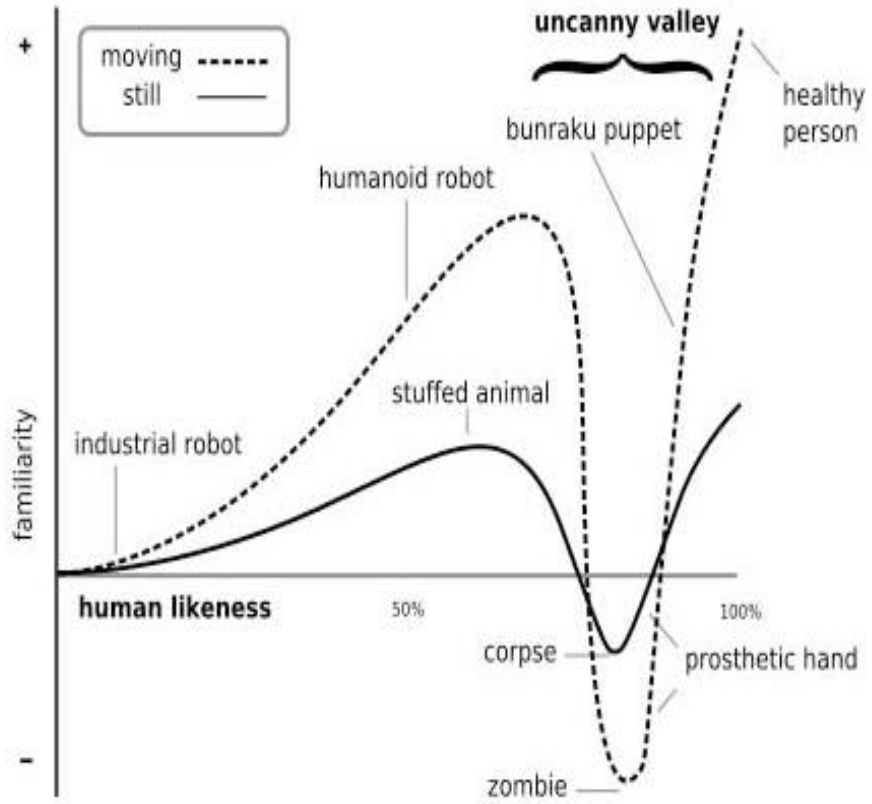
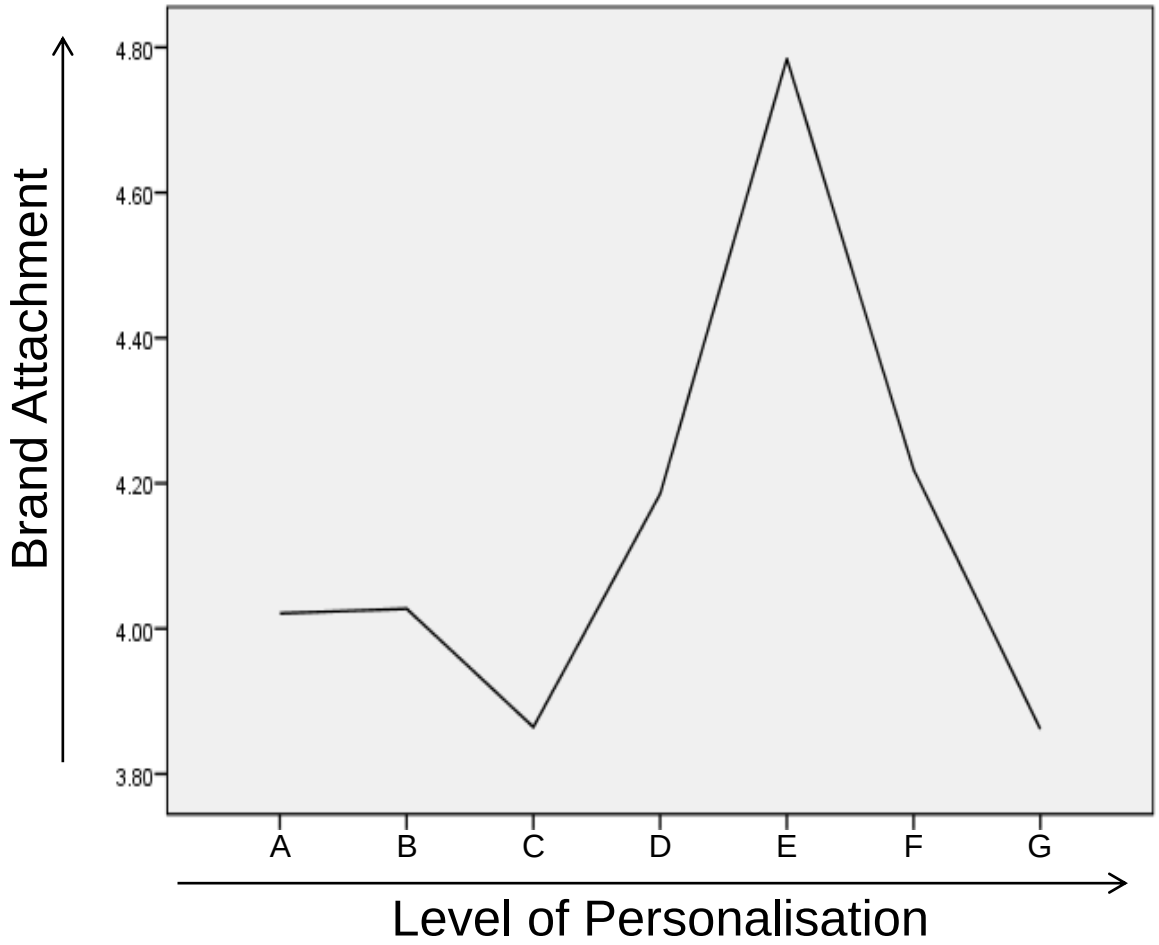


Chart by Masahiro Mori and Karl MacDorman



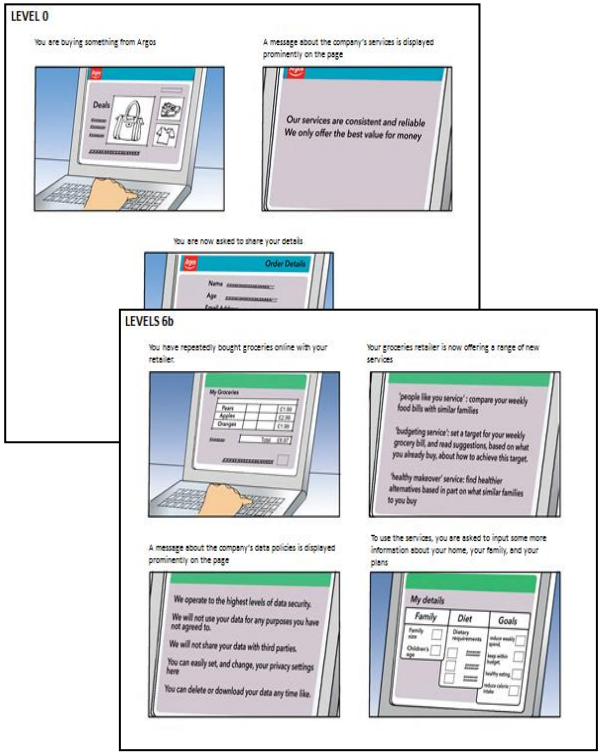


Instead of a linear relationship we found evidence of a serious drop-off in brand attachment after a certain point:



GfK researched how different approach to data sharing impact brand perceptions:

- Wanted to understand if different ways in which brands could overcome some of these obstacles
- Shown storyboards featuring online transactions
- Tested impact of giving assurances of company's data policies
  - Some no mention, others had explicit assurances
  - Tested in branded and unbranded contexts



Consumer willingness to share information:

+5%

Improvement in the likelihood of sharing information as a result of brand being specified

Ctrl Shift 2014

+12%

Improvement in the likelihood of sharing information when given assurances on data policies

Ctrl Shift 2014

-34%

Decline in the likelihood of sharing information when reminded of dangers of information sharing

Ctrl Shift 2014

Nudging privacy: Behavioural science provides insights into nuances of consumer behaviour around personal data

Availability heuristic

Risk assessment is influenced by information which is ready to hand

'Over assurances' created fall-off in willingness to share data

Ctrl Shift 2014

Control paradox

The illusion of greater control leads people to over-report

Fine controls on social networks led consumers to share more sensitive information with larger, audiences

GfK 2013

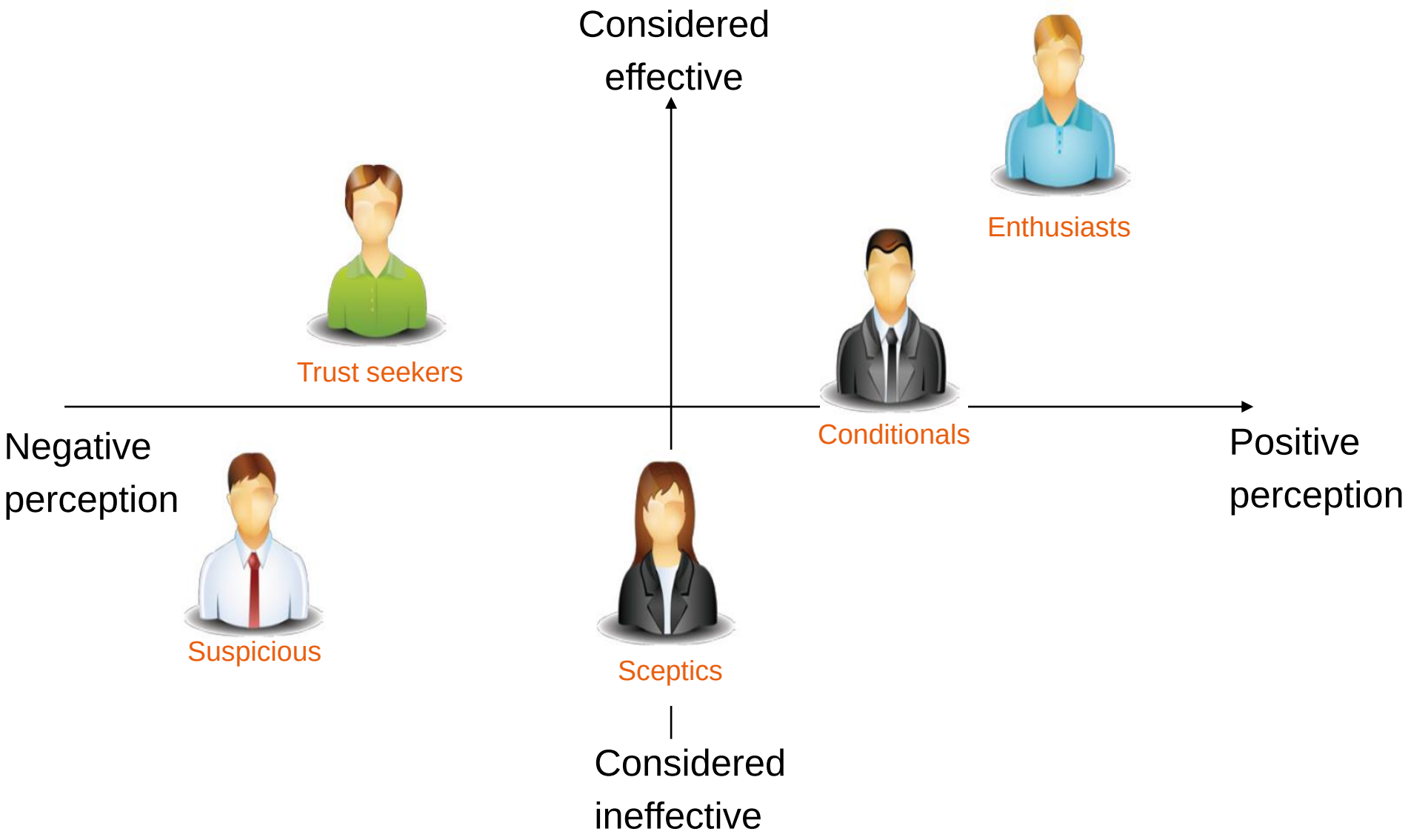
Coherent arbitrariness

When uncertain we will frame our response based on behaviour of others

When consumers reminded of dangers of indiscriminate sharing they perceive the brand more negatively

Ctrl Shift 2014

There is no one size fits all in attitudes to the use of personal data:



There is an appetite for greater engagement:

83%

Would like to know more about the information that companies hold on me

GfK 2014

86%

Would like greater control over what personal data companies hold on me

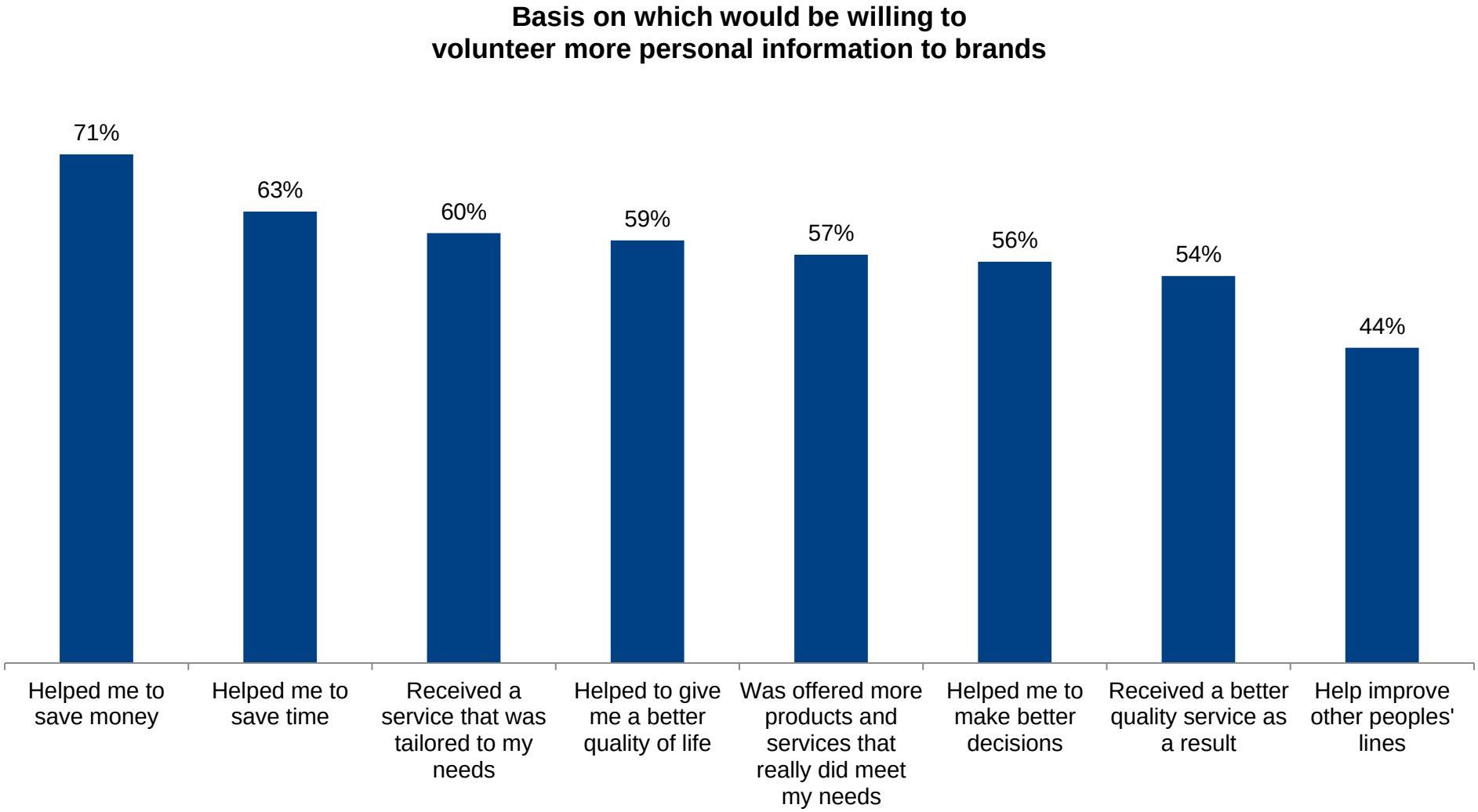
GfK 2014

77%

Would provide companies with more information if I could be sure they were not going to share it with anyone else unless I gave explicit permission

GfK 2014

Consumers are typically willing to consider volunteering more personal data if the value exchange is right:



This willingness to share data in return for genuine value is fuelling the personal data economy:











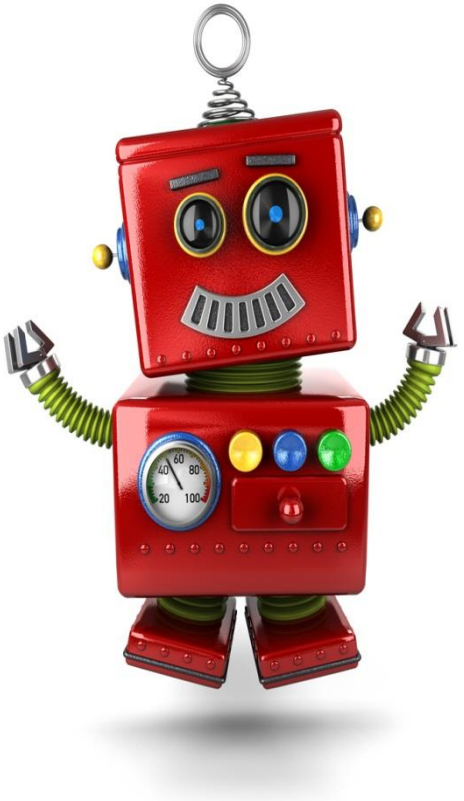






A call for new thinking:

- Consumer behaviour around personal data is complex and multi-faceted
- Challenge is to understand how to engage with consumers in a way that enhances rather than detracts from the brand
- Balancing act between providing transparency & control but also mindful of the pitfalls of consumer decision making in this area
- Attitudes are rapidly changing so more ongoing tracking is needed of changing consumer attitudes & behaviours



We'll cover

1. In market experience - MobileID and BankID (Nordics) — Janne
2. UK Banking and Mobile linkage — Sharon
3. "I'm in control", what the end-user wants — Colin

4. **Table breakout**
   a. What shape should AssureUK take for banks and mobile operators?
   b. What are the benefits of a central exchange vs. sector-specific exchange vs. bi-lateral data interchange agreements?
   c. What is the best next step?
5. Rapid fire feedback — All

We'll cover

1. In market experience - MobileID and BankID (Nordics) — Janne
2. UK Banking and Mobile linkage — Sharon
3. "I'm in control", what the end-user wants — Colin

4. **Table breakout**
   a. What shape should AssureUK take for banks and mobile operators?
   b. What are the benefits of a central exchange vs. sector-specific exchange vs. bi-lateral data interchange agreements?
   c. What is the best next step?
5. **Rapid fire feedback** — **All**

We'll cover

1. In market experience - MobileID and BankID (Nordics) — Janne
2. UK Banking and Mobile linkage — Sharon
3. "I'm in control", what the end-user wants — Colin

4. Table breakout
   a. what shape should AssureUK take for banks and mobile operators?
   b. What are the benefits of a central exchange vs. sector-specific exchange vs. bi-lateral data interchange agreements?
   c. What is the best next step?
5. Rapid fire feedback — All

6. AssureUK progress and forward plan

AssureUK Pipeline

Pilot	Sponsor	When	
		Dev	Launch
Age Verification Ticketing	Verizon/Miicard	Done	Available
Use Case: Comic Relief Gift Aid	Verizon/Piran	Now	tbc
Express Account Transfer	SecureKey	In discussion	As soon as needed
Mobile ID Federated Login	SecureKey	Feb	June
m-Banking passcode re-set using biometric authentication	The Human Chain	Feb	June
Verified SIM Card	Avoco Secure	May	Sept
m-Commerce Low and High Value Authentication	The Human Chain	May	Sept



THE HUMAN CHAIN

Passcode Reset Pilot 2014

From The Human Chain

Passcode Reset Pilot – What is it?

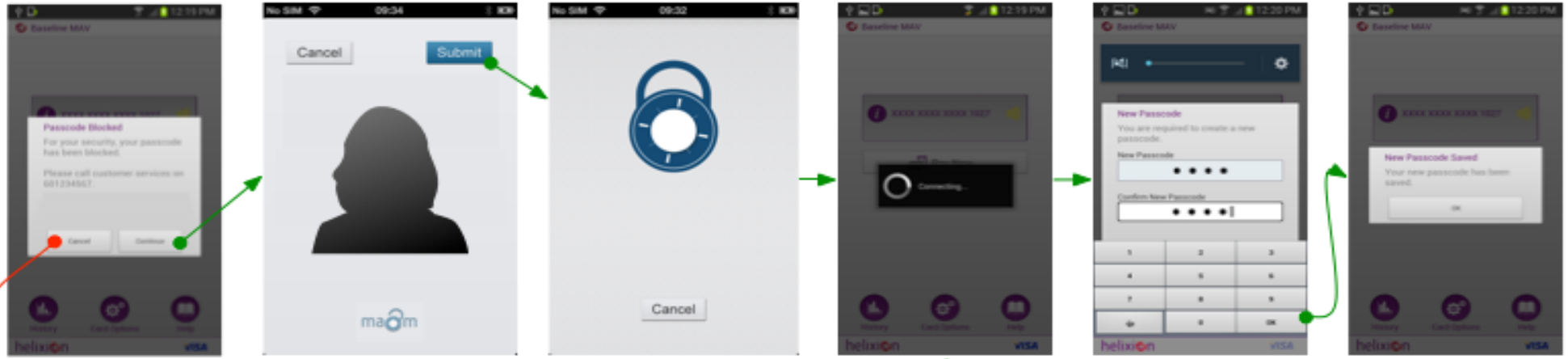
- **Purpose of Trial**
  - **Automate** mobile banking, contactless payment or MAV **app passcode re-set process** by using strong mobile biometric authentication mechanisms, reducing complexity, costs and improving security and convenience
- **How does it work?**
  - Customer clicks to initiate passcode re-set in mobile banking app, which initiates the re-set process
  - Seamlessly the Mobile Adaptive Authentication Manager (MAAM) screen opens and user is prompted to use either biometric (voice or facial recognition) authentication to identify themselves
  - Authentication data is authenticated by the MAAM processes and sent to the bank, which initiates a secure reset script, which then in app connects to the Visa Mobile Gateway (VMG) which prompts the end user to choose a new passcode
  - User completes re-set process and resumes full mobile banking app functionality
- **Benefits**
  - **Reduce complexity,** substantially **reduce costs** and greatly improve the mobile banking password re-set **user experience** by automating the process using the Visa Mobile Gateway (VMG)
  - **Improve security** by using strong mobile biometric authentication mechanisms
  - Provides all pilot participants with unrivalled knowledge/expertise and **first mover advantage** in mID

58

User Journey – Pilot

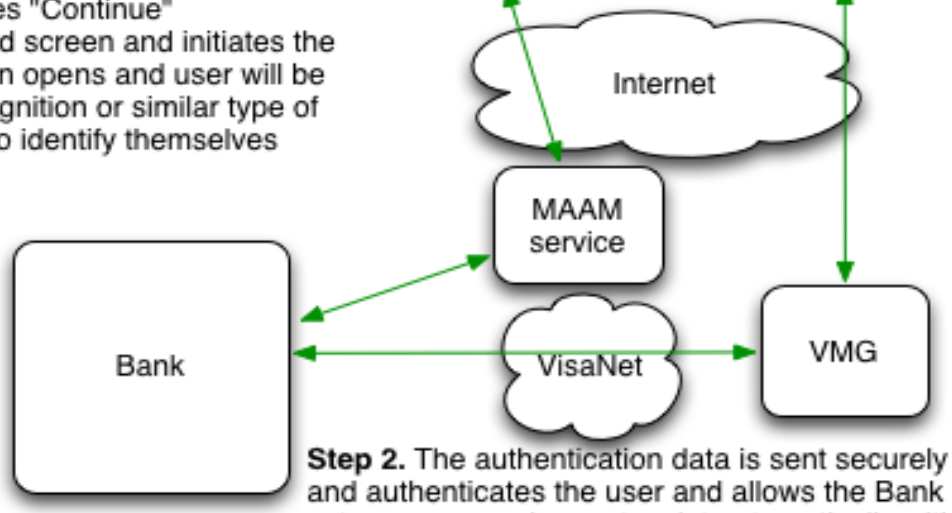
2. Mobile Adaptive Authentication Manager (MAAM) Biometrics Passcode Unblock Flow

2.1 Passcode blocked | 2.2 Authenticate using facial recognition | 2.3 MAAM processing | 2.4 Connection to VMG to reset | 2.5 Enter new passcode | 2.6 Passcode saved



Step 1. The user presses "Continue" on the passcode blocked screen and initiates the reset. The MAAM screen opens and user will be prompted for facial recognition or similar type of authentication method to identify themselves as the authorised user.

Cancel takes the user back to the home screen. Limited functionality available and payments disabled.



Step 2. The authentication data is sent securely to the MAAM system and authenticates the user and allows the Bank back end systems to set up a passcode reset script automatically without the need for the customer services step.

Step 3. Once the MAAM system has authenticated the user with the Bank and authorised the Passcode reset the app then connects to the VMG to complete the passcode reset process and the script is sent securely sent to the device.

Step 4. Once the passcode reset process has been completed the user is prompted to choose a new passcode and confirm it. The user can now resume making payments and using the full functionality of the app.

Passcode Reset – Work so far

- **Part of GSMA/OIX Assure UK Programme**
  - Passcode Pilot already selected for 2014 pilot programme
  - Agreed support from GSMA, Open Identity Exchange (OIX) and Cabinet Office (IDAP Programme)
- **Partners**
  - Payment Scheme – Visa
  - Issuer – tbc
  - Biometric Partner – Nuance
  - Identity Providers – UK Government accredited providers – Post Office, Verizon, Experian, Mydex & Digidentity
  - App and SDK Provider – Helixion
  - Technology Framework (MAAM) – The Human Chain
  - MNO – UK MNOs
- **Timeline**
  - Q1 2014 – Ramp Up
  - Q2-Q3 2014 – Pilot
- **Work still to do**
  - Formal engagement with issuing bank
  - Finalise pilot scope and deliverables

60

MAAM Contact

Tim Jefferson

The Human Chain Limited
Magdalen Centre
The Oxford Science Park
Oxford
OX4 4GA
United Kingdom

Mob: +44 7836 660 419
Tel: +44 1865 784 386
Fax: +44 1865 784 387

E-mail: timj@thehumanchain.com
Web: http://www.thehumanchain.com



61

SIM Card Registration Online Process

Using a verified identity

Copyright Avoco Secure Ltd 2014

Avoco Experience in this area

- Worked with government agency, DBCDE in Australia
- Large degree of fraudulent activity using pre-paid SIM cards
- Reduce fraud by registering SIM card only if verified
- In Australia used DVS system for online verification
- But could use any other verifying data source

Copyright Avoco Secure Ltd 2014

Identity AVOCO

AssureUK Pilot for SIM Card Registration

- **Benefits to the customer,**

- Customers go through registration process to achieve:
  - A verified identity that can be used to access Telco account and any other federated service / company through SSO
  - Activation of their SIM card

- **Benefits to the business?**

- SIM activation only occurs post verification of that customer. This means the business has verified address details which helps to prevent fraud and allows traceability of SIM cards used for criminal activities.

Copyright Avoco Secure Ltd 2014

Identity AVOCO

Added Value

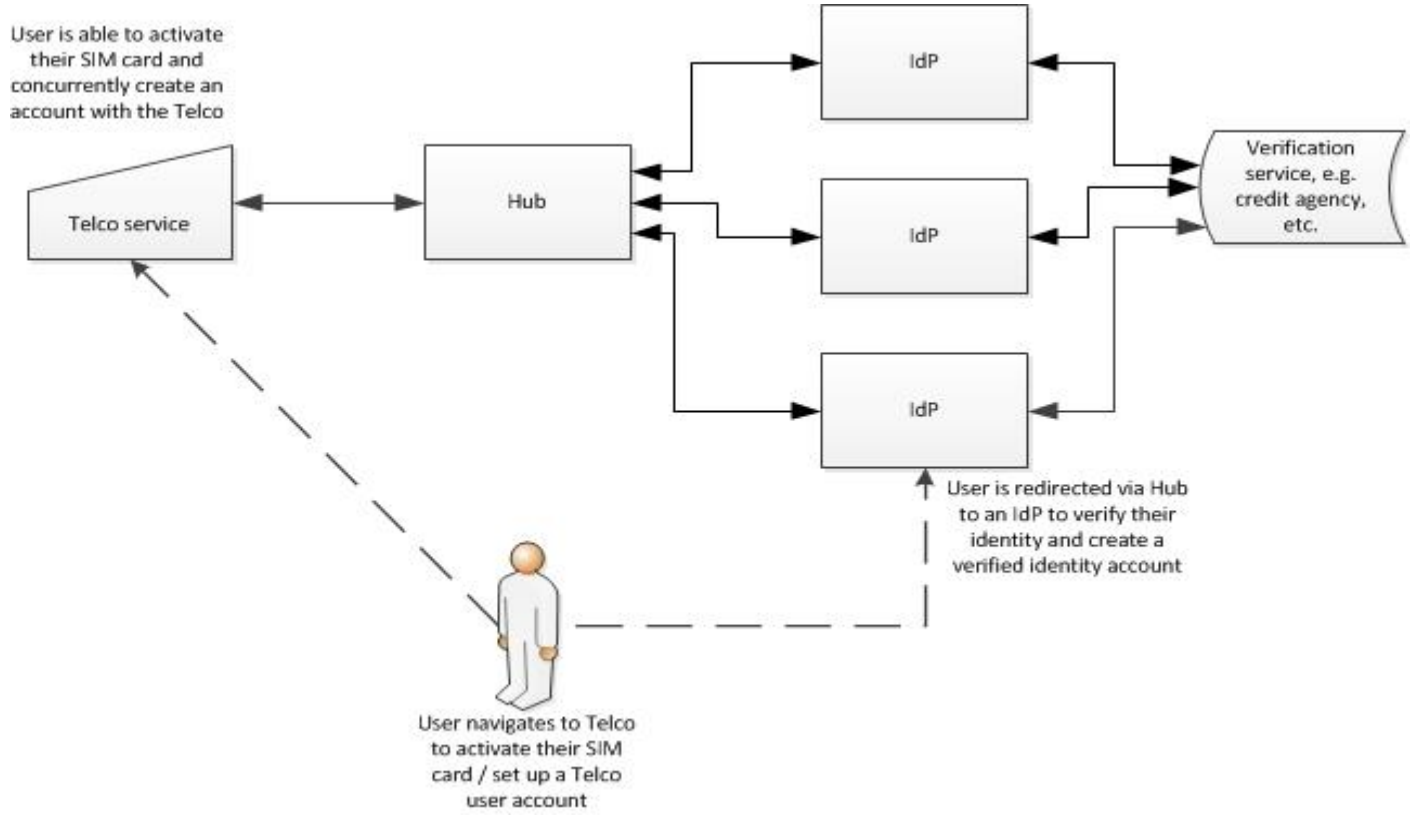
The verification process, not only allows that customer to activate their sim but it also has the potential to create them an account at the Telco

This account then:

- Creates a relationship between the customer and the Telco
- Allows the customer to use the same identity with other federated services
- Can offer SSO across those federated services
- And by doing so within the context of a wider data services platform (aka Trust Platform) can offer user consent models which build greater trust by giving users choices of who they share data with – ultimately this can be used to target marketing at the customer with their consent
- Other services such as user controlled credential management can be offered, which includes the ability to add their newly activated mobile number to their authentication options (both in SMS and mobile App form)
- The above can be sold as add on services to the basic identity

Copyright Avoco Secure Ltd 2014

Sim Activation Proposed Architecture (overview)



Copyright Avoco Secure Ltd 2014

Identity AVOCO

Where are we and what do we need?

- Currently working with SecureKey and Human Chain to reduce duplication of work, align with commercial market and support other GSMA pilots.
- Who else is prepared to work on this?
- Meetings with Telcos underway.

Copyright Avoco Secure Ltd 2014

We've covered

1. In market experience - MobileID and BankID (Nordics) — Janne
2. UK Banking and Mobile linkage — Sharon
3. "I'm in control", what the end-user wants — Colin

4. Table breakout
   a. what shape should AssureUK take for banks and mobile operators?
   b. What are the benefits of a central exchange vs. sector-specific exchange vs. bi-lateral data interchange agreements?
   c. What is the best next step?
5. Rapid fire feedback — All

6. AssureUK progress and forward plan — Andy
7. **Commuting**

GSMA – Personal Data

Andy Rudd +44 7860 400 950

arudd@gsma.com

OIX – UK Lead

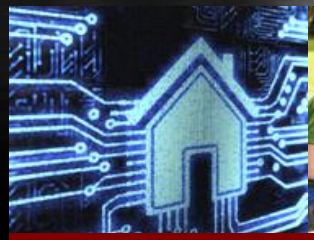
Sue Dawes +44 7786 391 243

Sue.Dawes@openidentityexchange.org



Connected Living















Connected Living – mTransport

Developing enablers for transport solutions in smart cities

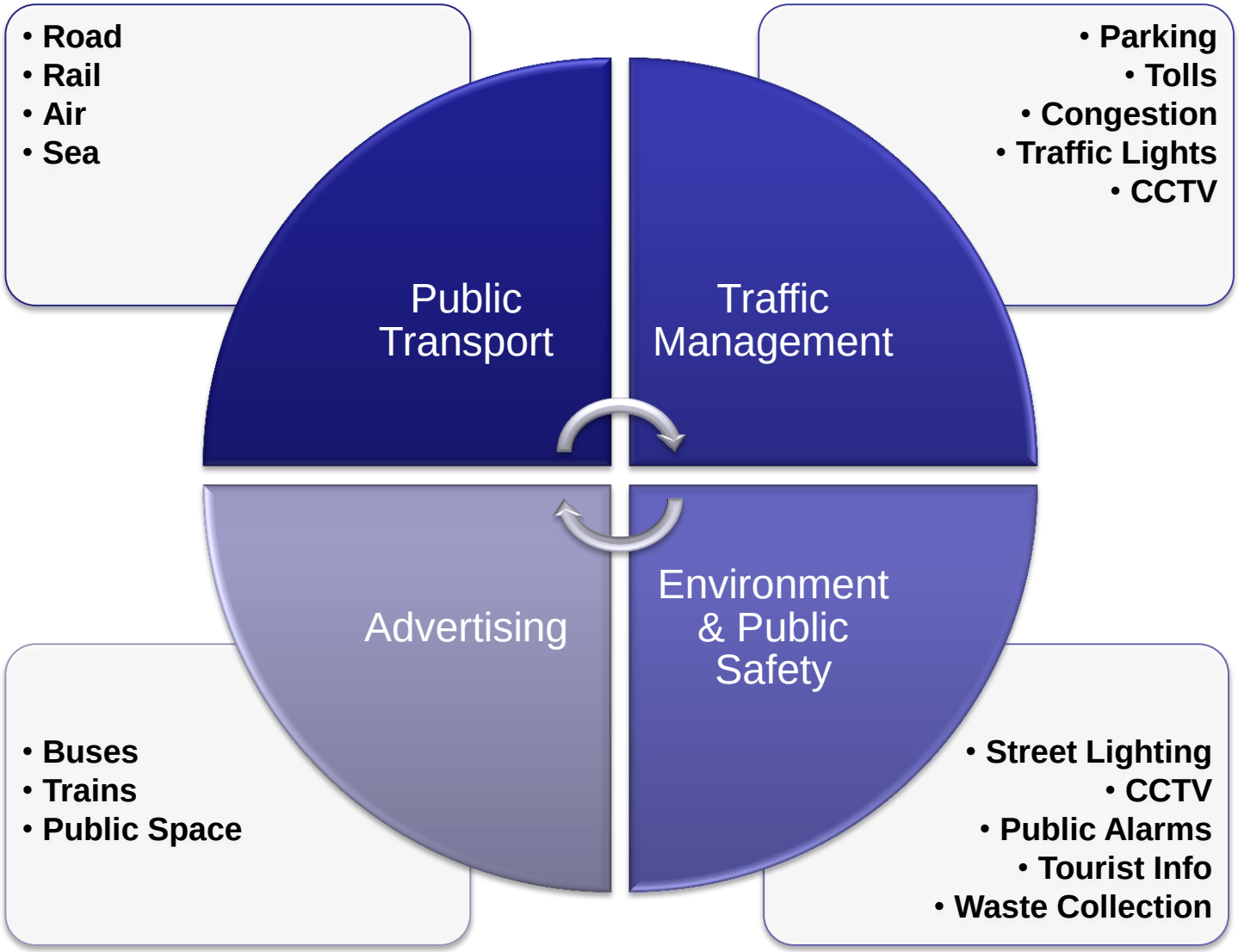
GSMA mTransport

Mobile Technology in Transport



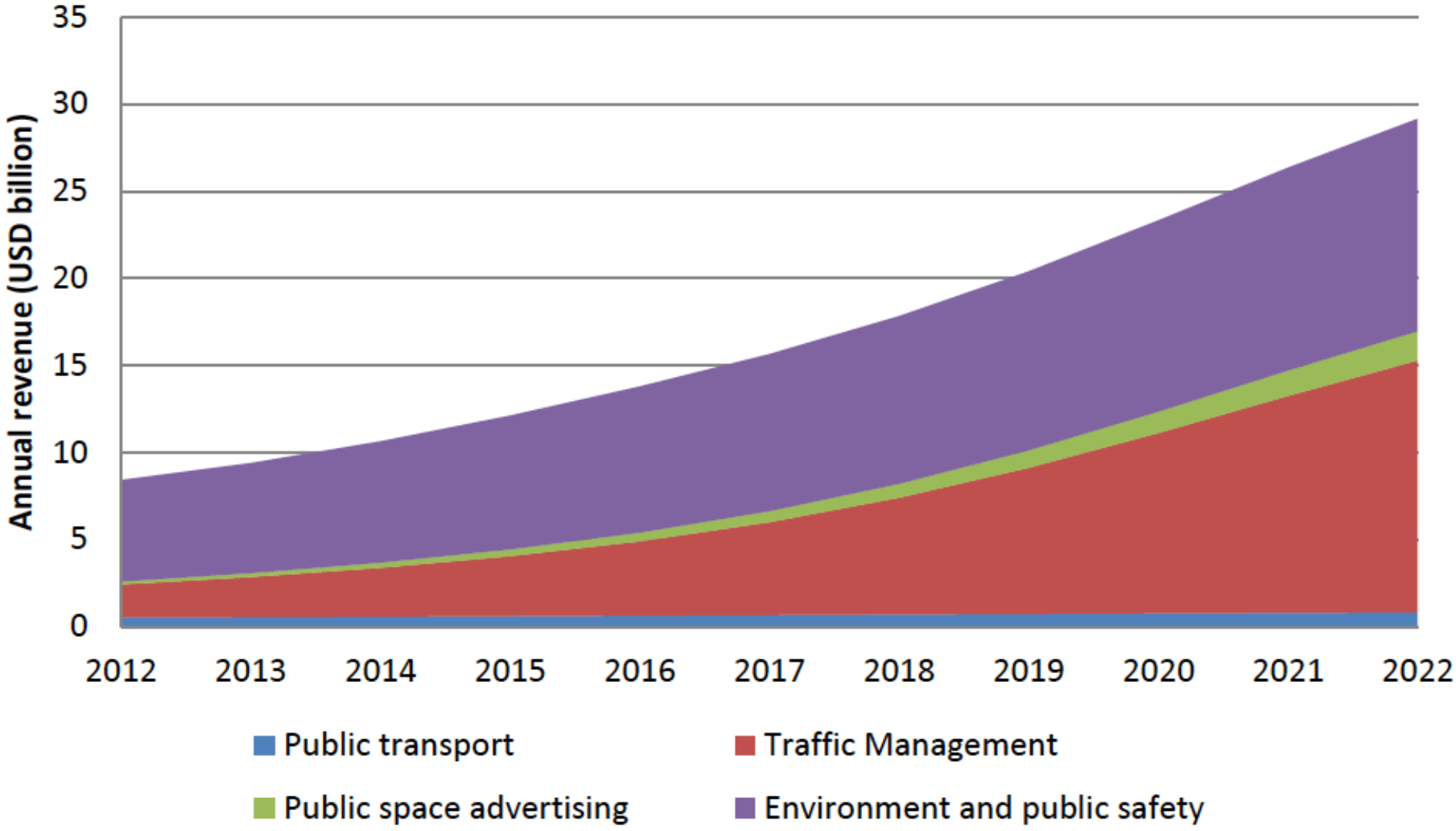
© GSM Association 2014

Scope of mTransport



© GSM Association 2014

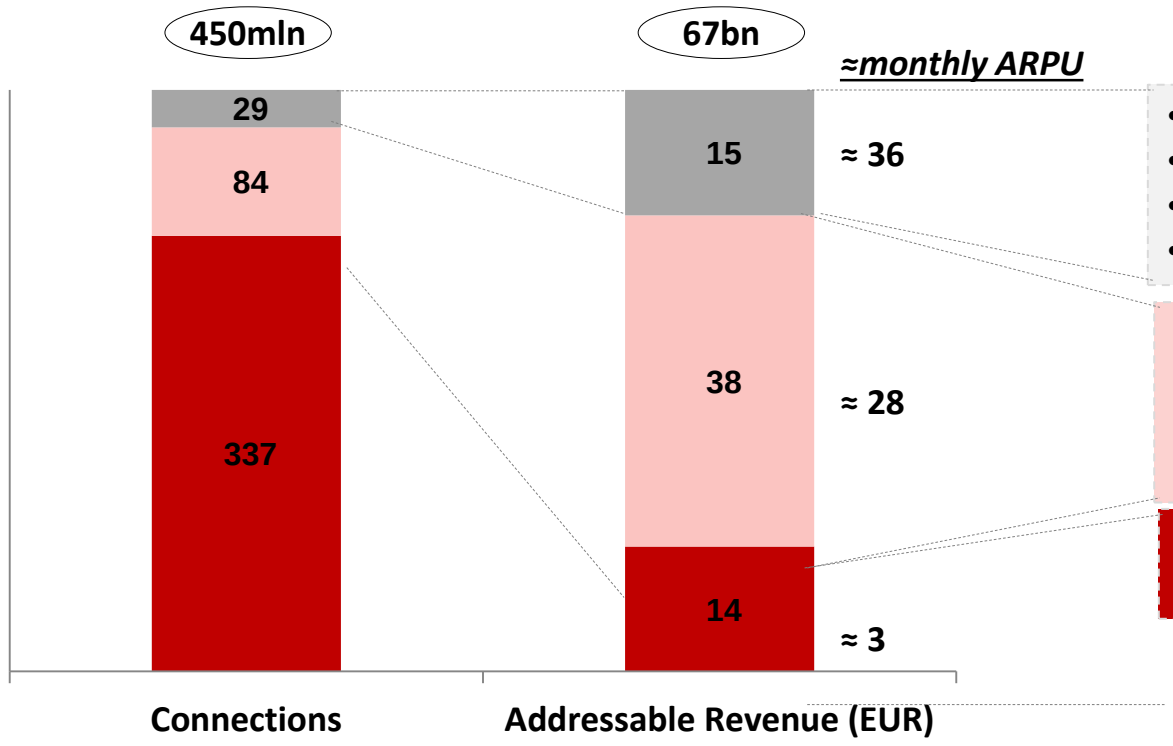
Global Revenue for M2M in Smart Cities and Transport 2012-2022 source: Machina



© GSM Association 2014

Smart city mobile opportunity of USD 67bn by 2020

Smart Cities market opportunity by 2020



Service categories

- Public space advertising
- Environment and public safety
- Public transport
- Traffic management

- Building automation
- LAN equipment
- Micro-generation
- Security

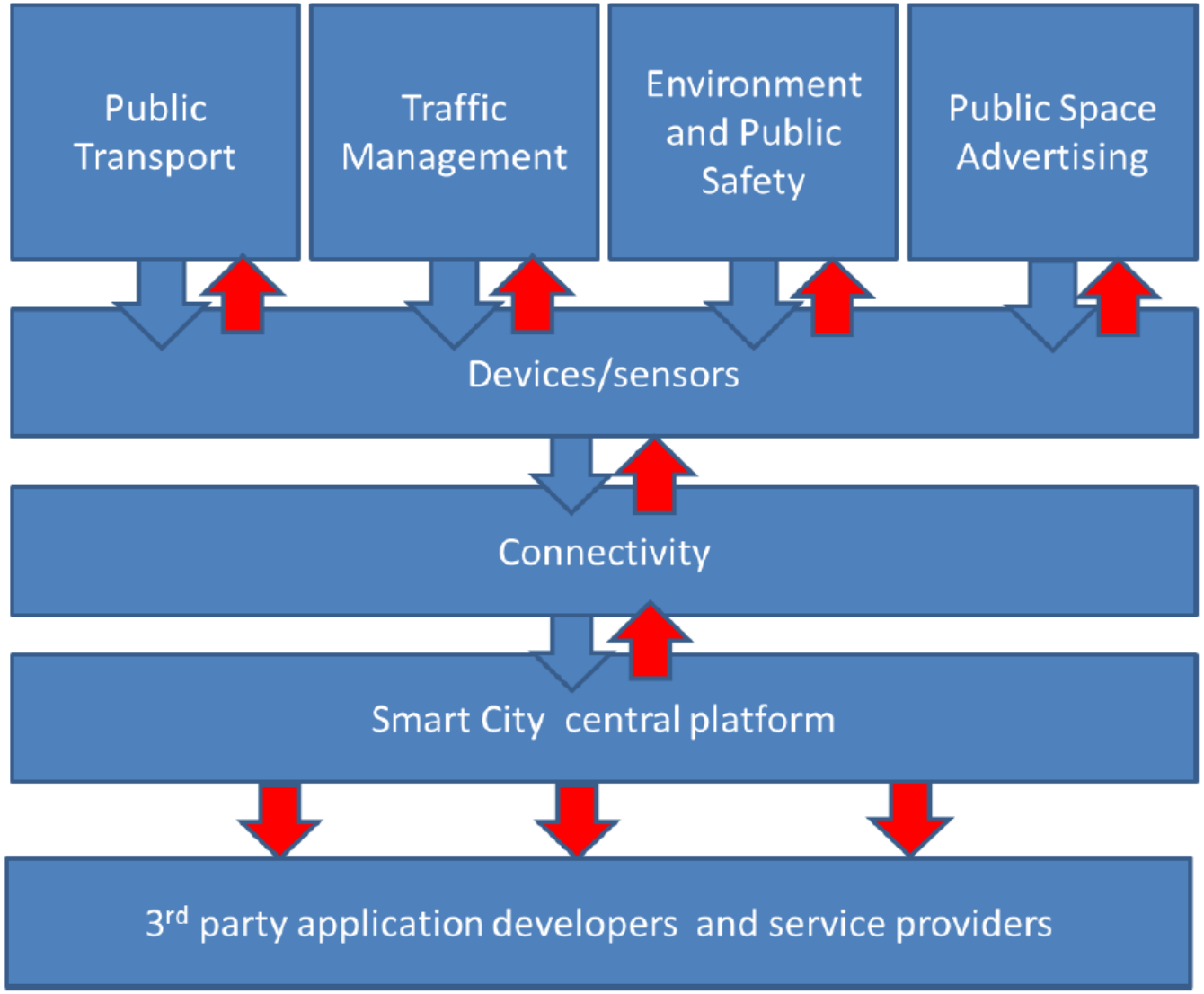
- Electric vehicle charging
- Smart metering

Wireless WAN connections (2G, 3G, 4G) and Mobile addressable revenue (USD)

Source: Machina, Utilities and Smart Cities reports

© GSM Association 2014

A central Horizontal Platform is required to manage Operations



© GSM Association 2014

eCall – European Union

- Mandatory in 32 countries
- All new model passenger vehicles from Sept 2015 must be fitted for eCall
- Currently 0.4% of vehicles are equipped
- By 2025 its expected 100% compliance
- Emergency Service Only
- Opportunity to provide other Value Added Services
- PSOP needs to be implemented nationally in all countries



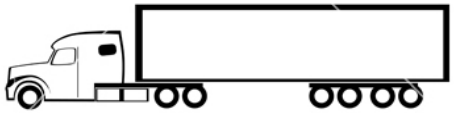
© GSM Association 2014

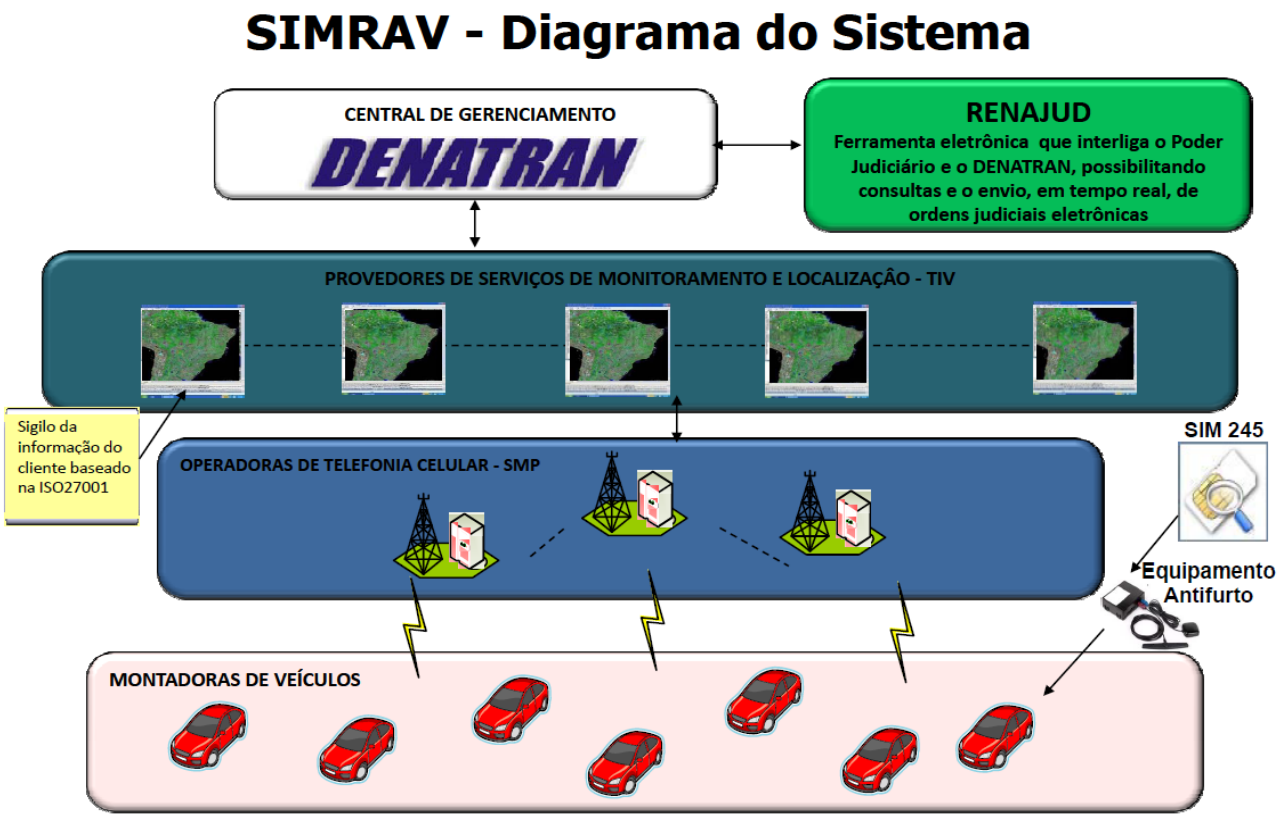
SIM RAV(DENATRAN 245) - Brazil

- Mandatory tracking for every private and commercial vehicle
- 25 Million Vehicles expected to be fitted by 2015
- Complex structure of service providers and services
- Strict Data privacy laws



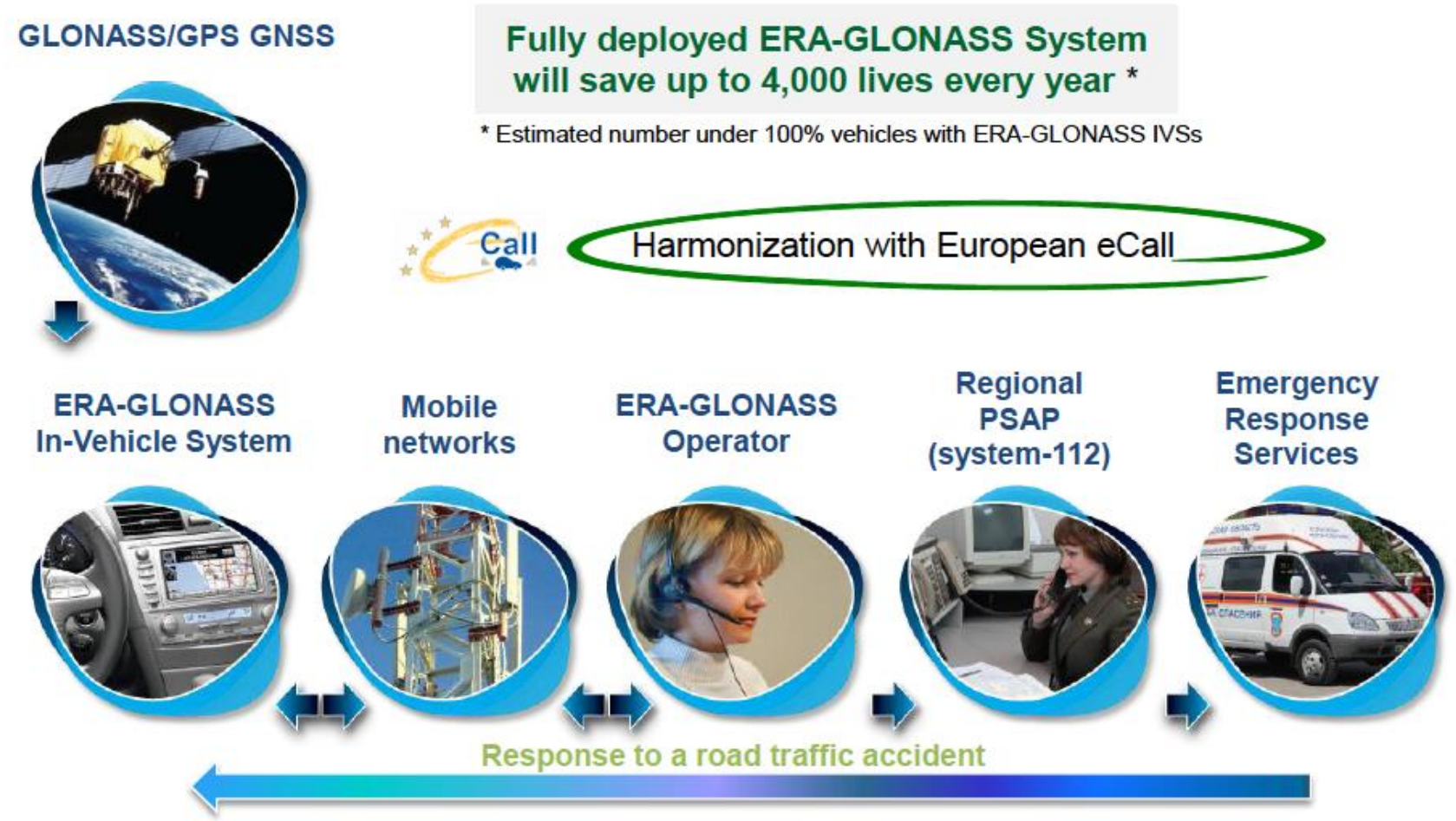






© GSM Association 2014

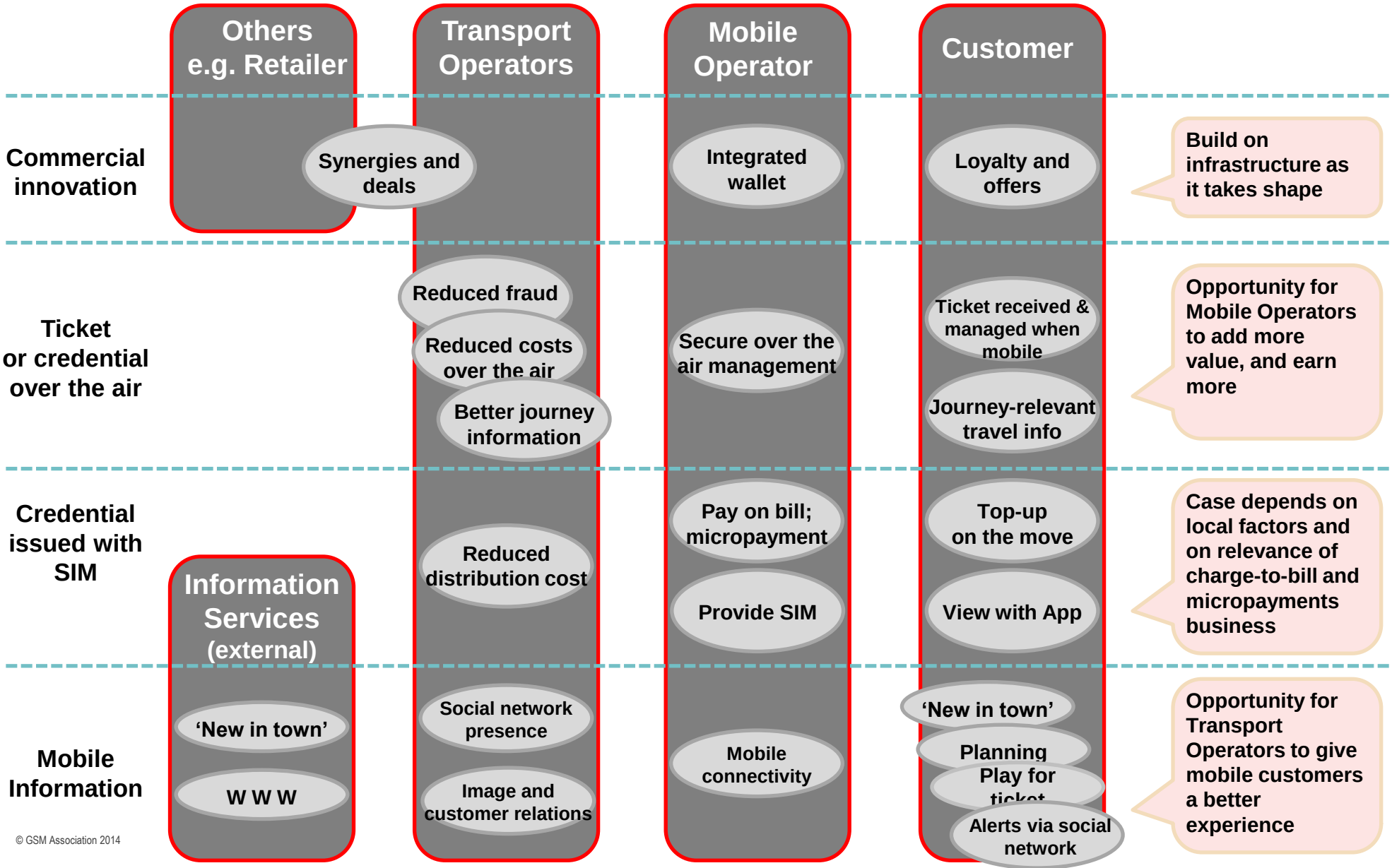
ERA Glonass - Russia



Implementation started in 2013 and phased for completion in 2015 and will save 8 Billion Rubles in Government costs annually when fully deployed

© GSM Association 2014

Role of Mobile in the Transport Value Chain



© GSM Association 2014

Case Study : Mobile Ticket in Russia

NOVOSIBIRSK
KAZAN

- 26 June 2013, “Mobile ticket” was launched by all Russian MNOs
- Service is available for ALL MNOs customers in region



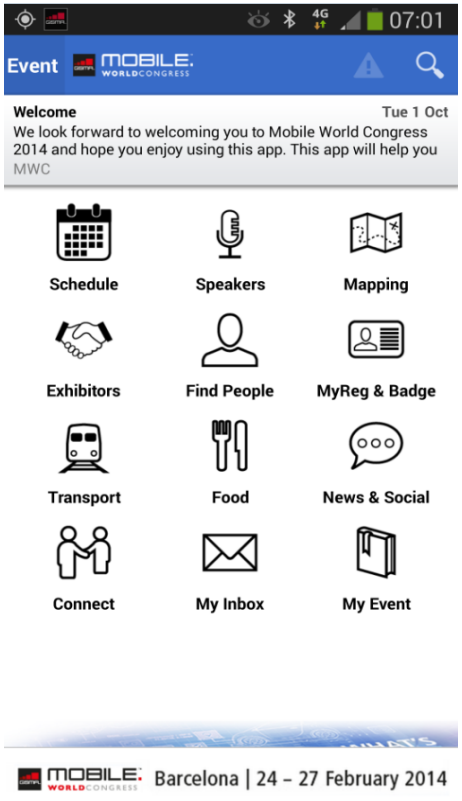
- Totally free of charge - no entry fee, no additional payments, free SIM-card
- Easy activation – just put SIM-card in your handset and reply via SMS
- Ticket’s price automatically charged from your mobile account when you tap special readers in the underground and buses
- Discounts – trips paid by “Mobile ticket” cost less than trips paid by cash

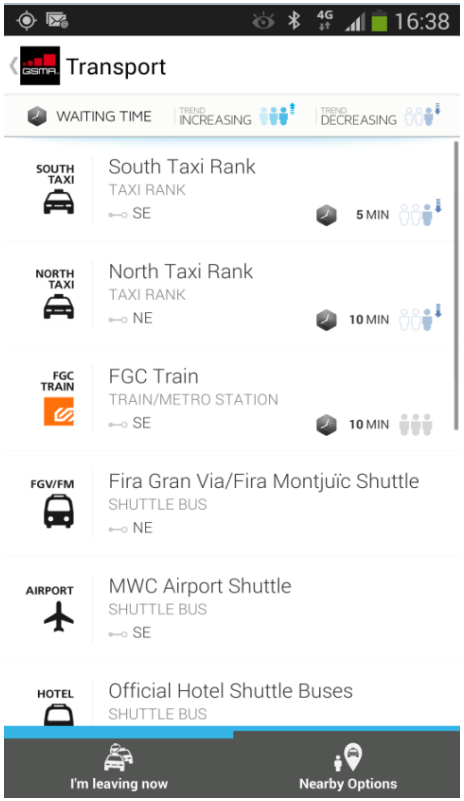


© GSM Association 2014

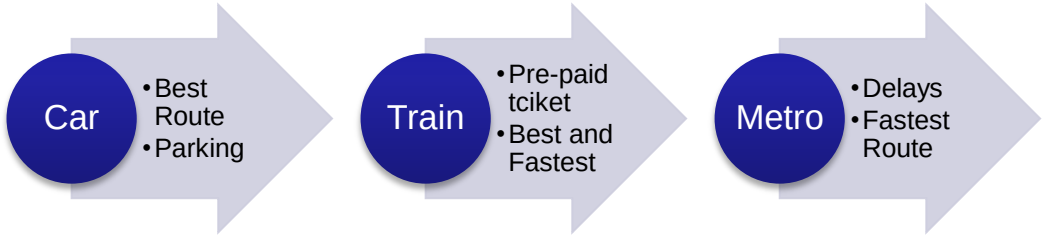
Apps for Events – a success story

- Plan your total journey before you leave
-
- Make the right decisions to get the best experience
- Customise to your interests
- Opportunity to use Big Data to enhance and improve efficiency







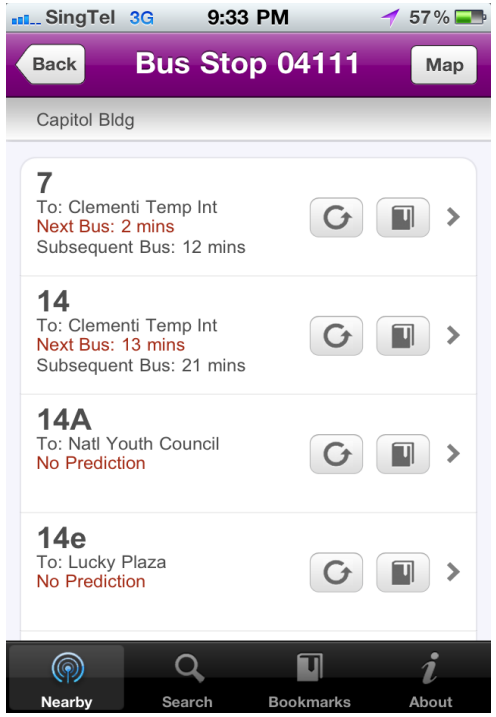


© GSM Association 2014

Integrated Public Transport Systems for Mobile Users





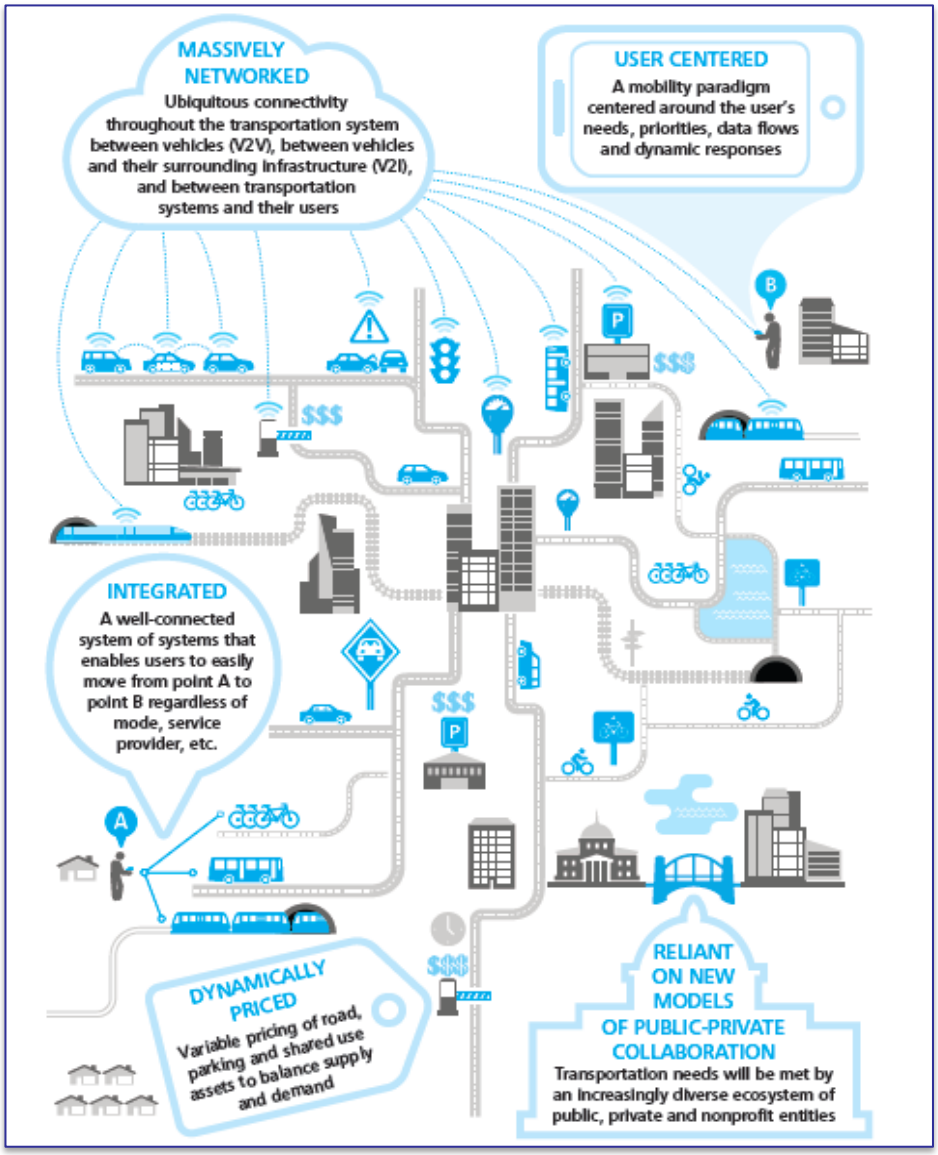


- Integrated Transit System
  - Bus , Train, Taxi
- Mobile Enabled Features
  - Route Schedules, Stop Schedules, Landmarks, Stop Finder, Real-Time Map
- Implemented in over 50 Cities

© GSM Association 2014

Key Features of Digital- age Transportation Systems

- User Centered
- Integrated
- Public-Private Collaboration
- Dynamic Pricing
- Ubiquitous Connectivity



© GSM Association 2014

Transport in Smart Cities – Latest GSMA's publications

Published 17 Feb 2014

GSMA Smart Cities

RTA du اتصالات etisalat

Smoother, Smarter Transport in the UAE

How mobile technologies are making it easier to travel on Dubai's metro, buses and water taxis

High-tech Dubai has become the first city in the Middle East in which people can use their mobile phones to access public transport.

Launched in September 2013, the new Smart NoI service enables a passenger to open a ticket barrier simply by tapping their handset against a reader. Instead of having transport credit stored on a conventional NoI plastic card, the new service enables the passenger to store credit on a virtual NoI account on the SIM card inside their handset.

When the consumer taps their phone against a ticket gate or an on-board reader, the service uses the short-range wireless technology NFC (Near Field Communications) to connect to the handset and validate the passenger's virtual NoI account. The passenger can use a NFC handset to check in and out of buses, metro stations and water taxis, prompting the appropriate fare to be deducted from their NoI credit.

Convenient and interactive

Developed by Dubai's Roads and Transport Authority (RTA) in conjunction with the Emirate's mobile operators Etisalat and Du, the groundbreaking service is designed to remove the need for passengers to carry a separate physical card. There are more than six million NoI cards in use in Dubai and, in time, the new service could significantly reduce the RTA's costs and environmental impact by removing the need to produce and distribute these plastic cards. The Smart NoI service is also designed to reinforce the high-tech, forward-looking image of Dubai's public transport (see box), further encouraging usage of the service.

For consumers, the service makes it easier to manage their NoI account: Passengers can review their NoI usage on their handset at anytime, anywhere, rather than having to use a machine in a metro station. The



passenger can use an Etisalat or Du app, or a special SIM toolkit menu, to check their current balance and the amount and date of their last NoI recharge (see boxes). They can also see the date and the cost of their most recent journey, whether they have reached the daily fare cap and their tag ID and expiry date, which a passenger needs when they contact the RTA call centre.

Passengers can top up the virtual card at RTA terminals or counters or online through the NoI web site using a unique number that appears on their display once the NFC SIM is placed into their smartphone. In future, Du plans to also enable its customers to use their mobile subscription to top up their NoI account.

New SIMs needed

Passengers need a NFC handset and NFC SIM card to use the Smart NoI service, which is preloaded with Dh 14 (almost 3 euros) of credit. Etisalat charges Dh25 (5 euros) to replace the SIM, plus an Dh50 activation fee and Dh5 monthly rental, while Du charges a flat rate of Dh55 for a SIM replacement, which will be supplemented by a NFC service fee of Dh2 a month from March 2014.

Public transport in Dubai

One of the world's fastest growing cities, Dubai has invested heavily in public transport in recent years. Formed by government decree in 2005, the Roads and Transport Authority (RTA) is responsible for both public transport and the road network in the Emirate of Dubai, and between Dubai and other Emirates of the UAE.

The Emirate's public transport systems combine metro, bus, road taxi and water taxis. The driverless metro system, which has 75km of tracks, is fully automated. It has two lines operational with a further three planned. The first urban train network in the Arabian Peninsula, the Dubai metro transported 33.2 million people in the first quarter of 2013, a significant increase over the same period the previous year.





GSMA PUBLISHES "EMBEDDED SIM" SPECIFICATION FOR MACHINE-TO-MACHINE (M2M) SERVICES

December 19, 2013 Press Release

Embedded SIM Initiative Aims to Accelerate the M2M Market Addressing Key Sectors Including Transportation and Utilities

London: The GSMA today announced the publication of its specification to enable the remote 'over the air' provisioning and management of Embedded SIMs in machine-to-machine (M2M) devices. The specification, which has the backing of the world's leading mobile operators and SIM suppliers, will help to ensure interoperable technical solutions and further accelerate the rapidly growing M2M market. First deployments of the GSMA-compliant Embedded SIM solution are expected to roll out in 2014.

"The number of mobile connected devices is expected to reach 11 billion by 2020, growth that will be led predominantly by advances in the M2M market," said Alex Sinclair, Chief Technology Officer, GSMA. "This level of growth will be heavily dependent on the adoption of a common, global and interoperable SIM provisioning and management architecture that enables the M2M market to flourish. The specification released today will have a significant impact on the M2M marketplace, as it will help provide lower operational costs and drive economies of scale."

© GSM Association 2014

Any other business

2014 Meeting Dates – Venue: GSMA

- Monday 24th March 2014 14.00 – 17.00

  Focus: Daily Banking transactions

- Thursday 19th June, 2014 14.00 – 17.00

  Focus: Daily Retail transactions
  - High Street, Online and Petrol forecourts

- Thursday 25th September 2014 14.00 – 17.00

  Focus: Monthly, seasonal or annual transactions
  - Utilities (metered domestic services) and entertainment ticketing (concerts, sport etc)
  - Insurance and Healthcare

- Thursday 11th December 2014 14.00 – 17.00

  Focus: AssureUK market reach, sector coverage and co-working
  - What are the next actions that ensure that the customer experience becomes more intuitive and convenient (but retains trust and security)

Register: oix.mvine.com sue.dawe@openidentityexchange.org

We've covered

1. In market experience - MobileID and BankID (Nordics) — Janne
2. UK Banking and Mobile linkage — Sharon
3. "I'm in control", what the end-user wants — Colin

4. Table breakout
   a. what shape should AssureUK take for banks and mobile operators?
   b. What are the benefits of a central exchange vs. sector-specific exchange vs. bi-lateral data interchange agreements?
   c. What is the best next step?
5. Rapid fire feedback — All

6. AssureUK progress and forward plan — Andy
7. Networking, cakes and tea — Lounge

GSMA – Personal Data
Andy Rudd +44 7860 400 950
arudd@gsma.com

OIX – UK Lead
Sue Dawes +44 7786 391 243
Sue.Dawes@openidentityexchange.org

