mobile connect

Secure digital identity is now in our hands

MOBILE CONNECT CONSUMER RESEARCH REPORT: EUROPEAN UNION

Personal Data

As the digital economy expands, individuals, businesses and governments are looking for ways to interact easily online without compromising security and privacy. The GSMA Personal Data programme aims to help digital service providers and consumers find the optimum balance between privacy, security and convenience. Working with its operator partners, the programme has developed and brought to market, Mobile Connect, the authentication and identity solution that provides a secure, seamless and convenient consumer experience, with a consistent user interface and low barriers to entry across the digital identity ecosystem.

gsma.com/personaldata

EIDAS Regulation

Mobile Connect has been specifically designed to comply with the European Union's eIDAS Regulation (Regulation on electronic identification and trust services for electronic transactions in the internal market), which is now being implemented by the 28 Member States. The Regulation, which introduces new rules on electronic identification services, is designed to enable citizens to carry out secure electronic transactions, such as enrolment in a foreign university and to access electronic health records, across the EU. It will also enable citizens moving to another Member State to manage registration and all other administration online with the same legal certainty as in traditional paper-based processes.

GSMA Intelligence

To gain insights into consumers' evolving attitudes to mobile and digital services, the GSMA Personal Data Programme commissioned KRC Research to canvas the views of smartphone users in the UK on personal data sharing, authentication to services and identification online. One of the main objectives of the research was to better understand how consumers will respond to Mobile Connect; a mobile operator-led service for secure authentication and identification of digital users and citizens.

The study, which combined an online survey of 1,000 smartphone users and a London-based focus group for face-to-face discussions, was conducted in February 2015. The KRC Research was supplemented by an online survey by TNS of 1,187 adults in the UK following the country's general election. That research was designed to establish citizens' views on using their mobile phones to verify their identity and vote in the context of an election.

The GSMA also commissioned Futuresight to ascertain service providers' perspectives on authentication, identification and Mobile Connect. Between March and May 2015, Futuresight conducted 50 qualitative telephone and in-person interviews with service providers, including 17 government agencies and banks, in the USA, UK, Germany, Singapore, Malaysia and India.

This paper, which summarises the key findings of these three pieces of research, is written primarily for governments and banks that could benefit from adopting Mobile Connect.

Contents

Executive Summary

Europeans are increasingly using their mobile phones to access a wide range of digital services, while governments, banks, merchants and other organisations are adopting a "digital & mobile first" approach to the design and delivery of services.

Yet as Europeans become more and more reliant on digital services, there is increasing dissatisfaction with log-in mechanisms that require them to remember multiple usernames and passwords and use a variety of security tokens. This frustration is combined with growing concern about the privacy implications of sharing personal data online. Both consumers and service providers are seeking a better authentication and identification solution, a demand that can be met by Mobile Connect, according to the findings of recent GSMA research.

Service providers are interested in Mobile Connect's potential to:

- **Accelerate and ease verification and authentication to make it easier to interact with consumers.**
- **Reduce friction (e.g. dropped logins, abandoned shopping carts) to increase registration and engagement.**
- **Enable access to operators' subscriber attributes (regardless of their operator) to provide better and more secure services.**

Governments and banks are particularly interested in using Mobile Connect to check attributes that can be indicators of fraud, such as an individual's location, while at the same time improving the end-user experience.

The research found three quarters of UK consumers would be likely to adopt Mobile Connect as their primary log-in for most websites, apps and online services. Almost 90% of the 1,000 smartphone users interviewed were attracted to Mobile Connect's three key propositions:

- **Universal log-in for multiple websites**
- **Strong security**
- **Control over personal data**

Together, the two studies suggest that widespread deployment of Mobile Connect by banks, government agencies and other service providers will increase usage of digital services by providing a simple and convenient authentication and identification solution.

mobile connect

Secure digital identity is now in our hands

gsma.com/mobileconnect

Challenges to the Digital Revolution

As people spend more time online, and as more services migrate to an omni-channel environment, access and security become more challenging:

38%
(of smartphone users)
Have weekly problems with logging in.

55%
(of smartphone users)
Say online privacy is a major concern.

2.4M
Customer details stolen at Carphone Warehouse - just the latest in a long line of security breaches

Source: http://www.telegraph.co.uk/finance/newsbysector/epic/cpw/11791988/Carphone-Warehouse-hackers-gain-access-to-bank-details-of-2.4-million-customers.html

The answer to secure digital authentication is in our hands

INTRODUCING:

Mobile Connect Log-in

The new standard of digital authentication with privacy protection, developed by the GSMA and its operator partners. By simply matching people to their mobile phone, Mobile Connect provides secure access to website and apps without multiple passwords and usernames.

77%
Feel their personal data is secure with their mobile operator

88%
Find a 'Universal' log-in appealing for multiple websites.

88%
Think stronger online security is appealing.

Secure access

By solving the challenge of secure access to digital services, whilst protecting consumer privacy, the potential and adoption of further digital services emerges, unhindered. In the consumer survey uses predicted to use smartphones for by 2020 included:

53% Believe they will be making online payments using their mobile phone without cards.

49% Believe they will store tickets for travelling on their mobile phone

30% Believe they will be using their phone to actively protect themselves from fraud

Mobile identification

Even today, mobile identification can provide a channel for greater engagement:

72% OF VOTERS

(18-24 year olds) in the 2015 UK general election would have been happy to prove their identity using a mobile device.

Of those who didn't vote, 40% said that they would have done so if they could have voted via a mobile device. That figure rose to 55% among 18-25 year olds.

68% of the respondents agreed the UK should use the latest technology to make voting easier and less open to fraud.

1. Digital challenges facing individuals and service providers

Growing demand for and reliance on digital services

In Europe, consumers are increasingly using mobile phones to access a wide range of digital services. In the UK, for example, 22% of smartphone users spend more than three hours a day accessing the Internet from their phones, according to the GSMA's research.

Over time, UK consumers expect their handsets to take on an even more central role in their lives. Within five years, approximately half of the respondents in the online survey said they expect to be using their mobile phone to perform daily tasks, such as making payments, storing loyalty cards and coupons, and as a ticket for travelling on public transport (see Table 1).

TABLE 1: WHAT DOCUMENTS OR PROCESSES DO YOU EXPECT TO STORE, OR CARRY OUT, USING YOUR MOBILE PHONE BY 2020?

Making a payment to an online store without cards	53%
Storing loyalty cards and coupons	49%
Tickets for travelling on public transport	49%
Authorising access to home Internet and TV	37%
Voting in elections	34%
Actively protecting yourself, your home and family from hacking and fraud	30%
Storing your driving license	29%
Registering or sharing information with your doctor	28%
Proving your age when purchasing alcohol or cigarettes at a self-service check out	25%
Entering a country using a passport	22%
Entering your place of work, VPN, printers etc.	20%
Filing your tax returns	20%

At the same time, banks, merchants, governments and other online service providers are increasingly adopting "mobile-first design" (prioritising the mobile user experience) for their digital services. In interviews commissioned by the GSMA, the service providers said there is an increasing need and desire for end-users to log-in and transact via mobile.

1. GSMA Intelligence, Sept 2015

Individuals' challenges and concerns

But even as consumers become increasingly reliant on their mobile phones and digital services, there is dissatisfaction about the steps they are required to take to access these services and their lack of control over their data and privacy.

The consumer research found that many people struggle, for example, to complete the log-in process employed by websites and apps; more than one third (38%) of UK smartphone users said they encounter problems logging into online services on a weekly basis. The study suggests that 90% of UK consumers would like to move away from having to remember multiple different usernames and passwords.

There is also growing concern in the UK about the privacy implications of the increasingly digital and data-driven economy. In the consumer study, 55% of the respondents agreed with the following statement: "Online privacy and security is a major concern of mine and I do everything I can to make sure I'm protected."

Many digital services require consumers to share some information about themselves and two thirds of the respondents said they are "ok letting companies know a little about me in exchange for access to services or products." However, consumers' comfort levels vary with the type of data being shared. For example, 76% are comfortable sharing data about their shopping and purchasing needs in exchange for deals and other benefits, but only 50% felt the same about sharing details of their device, such as the reference numbers of their handset, operator account and SIM card (see Table 2).

55% STATED THAT:

"Online privacy and security is a major concern of mine and I do everything I can to make sure I'm protected."

TABLE 2: % COMFORTABLE SHARING DATA ABOUT THEIR:

	....in exchange for deals and other benefits
Shopping & purchasing needs	76%
Personal interests and preferences	74%
Electricity, gas and water bill/usage data	73%
Websites visited	65%
Network data: operator's name, phone location, roaming country	61%
Personal data: name and address, mobile number, email address, dob	56%
Phone account data: contract type, payment history	54%
Device details: technical details and reference numbers of your handset, operator account, and SIM card	50%

Governments' and banks' challenges and concerns

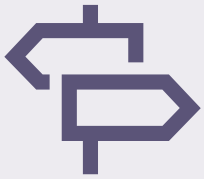
Although they are prioritising the mobile channel, service providers say the small form factor of handsets and other user-experience constraints are holding back engagement and registration – an issue frequently referred to as "friction". In the interviews commissioned by the GSMA, the service providers also acknowledged growing awareness among consumers of the value of personal data, particularly in developed countries, and the importance of explicit consent in some sectors, as well as the need to give consumers value in return for sharing their data.

For governments and banks, the need for high levels of security can further increase the friction involved in online interactions with individuals. For this reason banking and financial services generally require implicit consent specifically to maintain a high quality user experience in a high security environment. Service providers in these sectors highlighted their need for consumers' implicit consent to use personal data for various purposes, such as fraud reduction, the exchange of credit-scoring information between banks and government security, planning and resourcing.

Service providers have reported increasing difficulty in gaining end-user consent to use personally identifiable data for marketing and profiling purposes. There was broad acceptance that consent must be transparent and generally explicit, given that consumers can typically switch to another service provider, and given the need to protect the service provider's reputation and maintain trust. Overall, service providers say that respect for privacy and maintaining a good user experience is increasingly important.

One of the biggest challenges identified by service providers is striking the right balance between obtaining explicit consent and irritating end-users with repeated requests, which create friction and slow down the interaction. The consensus was that explicit 'one-time' consent, coupled with an explicit and transparent method of 'opting out', is the best way to achieve that balance. Ironically, some service providers believe consumers are less likely to opt-out if they think it is easy and simple to do so.

One of the biggest challenges identified by service providers is striking the right balance between obtaining explicit consent and irritating end-users with repeated requests, which create friction and slow down the interaction.



2. What do citizens want?

Greater convenience

There is very strong latent demand for a more convenient means of logging in securely to online services. Nine out of ten of the respondents in the consumer survey in the UK would welcome a single log-in solution - a username and password that they were confident were secure - for all or most websites. More than half (54%) said such a solution would be "very beneficial".

Younger people, in particular, are comfortable using their mobile phone to authenticate or identify themselves. In the TNS survey of UK adults, 72% of the 18-24 year olds who voted in the May 2015 UK general election would have been happy to prove their identity using a mobile device, such as a tablet or smartphone. Moreover, almost two-thirds of respondents aged between 25-34 year olds would also have been comfortable using their handset to prove their identity.

Among those who didn't vote, 40% said that they would have done so if they could have voted via a mobile device. That figure rose to 55% among 18-25 year olds. Across the entire sample, 68% of the respondents agreed (37% strongly) that the UK should use the latest technology to make voting easier and less open to fraud.

Greater control

If individuals feel like they are in control, they are more likely to interact online and share relevant personal data. Almost seven out of ten (69%) of the respondents in the consumer survey said they would be likely to share information on their shopping and purchasing needs if they could control what data was shared with which advertiser, to make the ads they see online more relevant to them. A similar proportion said they would be likely to share information on personal interests and preferences on the same basis.

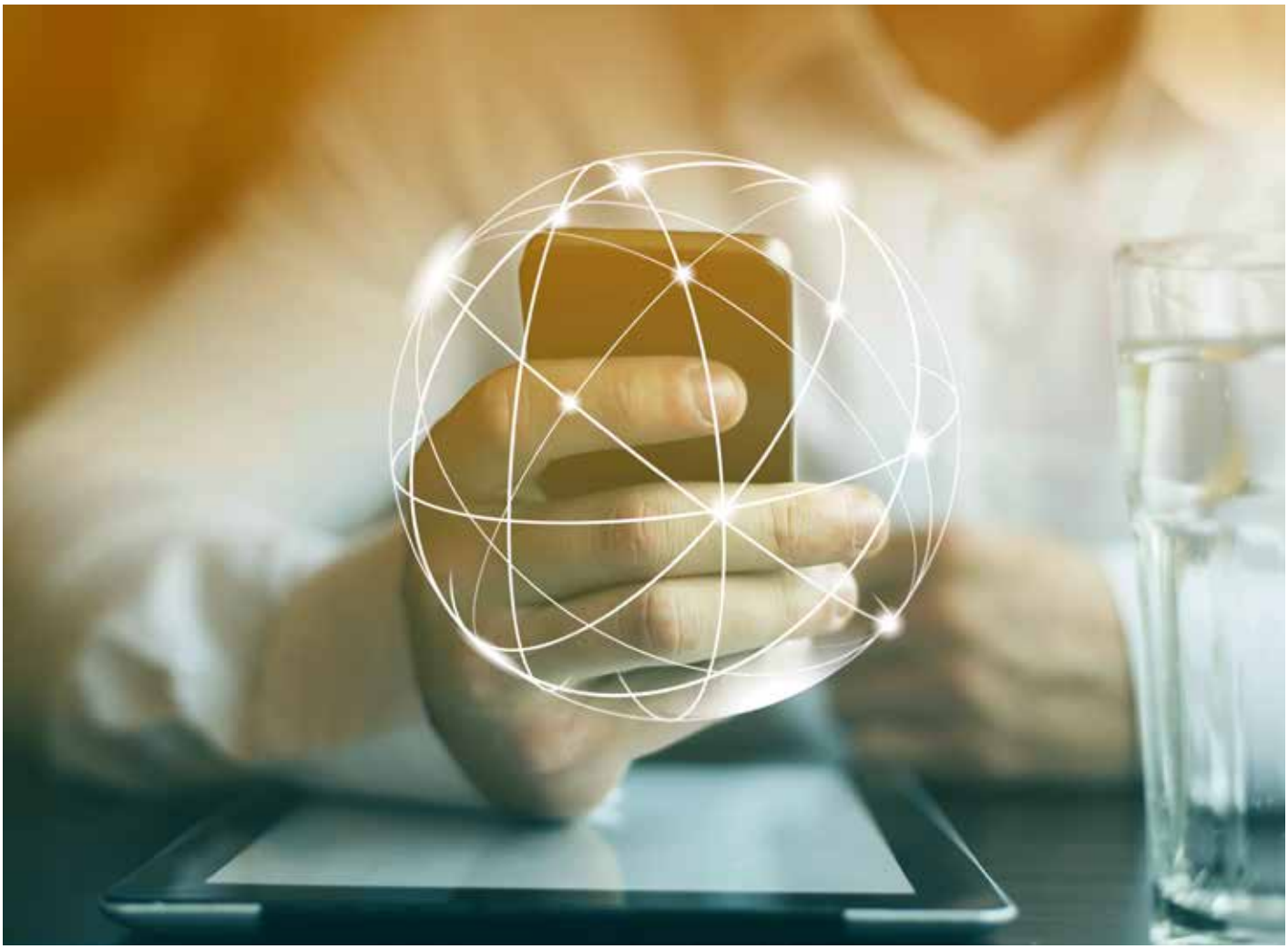
Nine out of ten of the respondents in the consumer survey in the UK would welcome a single log-in solution - a username and password that they were confident were secure - for all or most websites.

Among those who didn't vote, 40% said that they would have done so if they could have voted via a mobile device. That figure rose to 55% among 18-25 year olds.

3. Introducing Mobile Connect

Developed by the GSMA with a lead group of mobile operators, Mobile Connect is a secure authentication and identification solution. It provides:

- **Simple, secure access which leverages the inherent security of network assets via the individual's mobile phone for authentication.**
- **Support for anonymous log-in with control over what personal information is shared.**
- **An alternative to multiple passwords and access mechanisms, which can consistently be used at different security levels.**



Governments' and banks' initial response to Mobile Connect

There was exceptionally high interest in Mobile Connect among the majority of service providers interviewed in the GSMA study. In particular, service providers were interested in Mobile Connect's potential to:

- **Accelerate and ease verification and authentication to make it easier to interact with consumers.**
- **Reduce friction (e.g. dropped logins, abandoned shopping carts) to increase registration and engagement.**
- **Enable access to services that utilise subscriber attributes (regardless of their operator) to provide better and more secure services.**

The service providers welcomed Mobile Connect's potential to reach all of their customers across national boundaries and jurisdictions rather than just a subset. They were also very positive about the solution's ability to support authentication and identification, as well as the potential to enable users to control sharing of their personal data from any platform or device.

The service providers welcomed Mobile Connect's potential to reach all of their customers across national boundaries and jurisdictions rather than just a subset.

Banks and governments liked Mobile Connect's ability to provide attribute services that can enhance verification in order to fight fraud.

The research suggests there is likely to be particularly strong demand for Mobile Connect from government agencies and banks from many countries. In these sectors, which generally face the biggest challenges in terms of identity and friction, there is a clear need for better verification mechanisms. Banks and governments liked Mobile Connect's ability to provide attribute services that can enhance verification in order to fight fraud. For example, a bank could use Mobile Connect to double-check that a particular individual is actually initiating a transaction (see next section for more detail).

Governments and banks are also very interested in Mobile Connect's ability to increase transparency and make it simple for individuals to opt-out, thereby supporting the credibility of implicit consent in the eyes of the consumer.

Individuals' initial response to Mobile Connect

The Mobile Connect proposition also resonates with consumers. Participants in the consumer survey in the UK watched a video describing the Mobile Connect solution. They were then asked how likely they would be to use Mobile Connect as their primary log-in for most websites, apps, and other online services. The response was very positive: 25% said very likely and 50% somewhat likely.

The research drilled down further on the three key aspects of the Mobile Connect proposition:

1) **Universal or single log-in for multiple websites**
2) **Strong security**
3) **Control over personal data**

All three of these value propositions resonated with UK smartphone users (see Table 3)

TABLE 3

	Very appealing	Somewhat appealing
Universal log-in: Mobile Connect enables you to easily login to multiple websites using your mobile phone, and just one password for them all	**47%**	**41%**
Strong security: Mobile Connect provides stronger security than current log-in systems thanks to the unique combination of your phone and its password	**43%**	**45%**
Control over personal data: Mobile Connect allows you to log-in anonymously or those services that do not require to know your identity.	**46%**	**43%**

Universal log-in for multiple websites

Mobile Connect's potential to enable individuals to log-in to multiple websites using a mobile phone, and just one password for all the sites, resonated with 88% of the UK consumers surveyed (see Table 3). Almost half of the respondents found this proposition very appealing.

Strong security

Almost nine out of ten (88%) of UK smartphone users welcomed the Mobile Connect promise to deliver stronger security than current log-in systems through the combination of the consumer's phone and a PIN – two-factor authentication (see Table 3).

The research also highlighted UK consumers' worries about identity theft and associated fraud. By utilising mobile operators' secure network assets, Mobile Connect is able to provide advanced protection against identity theft and secure and reliable identity verification. These features appealed to almost 90% of the people participating in the survey (see Table 4).

TABLE 4

	Very appealing	Somewhat appealing
Mobile Connect provides advanced protection from the growing threat of identity theft	**47%**	**42%**
Mobile Connect provides a more secure verification of your identity - proving you are the real you	**43%**	**45%**

Control over personal data

The study found strong latent demand among UK consumers for a service that could give them greater control over their personal data. When they were introduced to the Mobile Connect proposition, 89% of respondents liked the idea of being able to manage permissions for sharing their personal data with online services (see Table 5).

Most of the respondents also found the concept of a personal data vault that allows the user to collect, manage and control their personal information to be appealing. There was even more enthusiasm for a consistent set of privacy guidelines across service providers (see Table 5).

TABLE 5

	Very appealing	Somewhat appealing
Mobile Connect allows you to manage permissions for sharing your personal data with online services.	**43%**	**46%**
Mobile Connect creates a personal data vault that allows you to collect, manage and control your personal information	**39%**	**46%**
Mobile Connect's partner services must adopt the same set of privacy guidelines, reinforcing your privacy and control	**46%**	**42%**

4. Example use cases

In the consumer survey, UK smartphone users were presented with various scenarios in which Mobile Connect could be used. The vast majority of respondents were interested in these use cases (see Table 6).

TABLE 6: % TOTAL INTERESTED

Reduced risk of identity theft and credit card fraud by increasing the security of all your financial transactions online and in the store because your bank and payment providers can quickly check with you	**89%**
For almost all login scenarios, just one strong password to remember that delivers high security, instead of having to remember dozens of potentially weaker passwords	**88%**
Real-time parental control of your family's login to online services	
Shorter wait times or queues and better service at call centres, enabled because mobile connect allows you to pre-identify yourself	**83%**
Easier and more secure authorisation of online banking transactions without the fuss of using 'card devices', and filling in long forms to prove your identity	**82%**
Auto-fill online registration forms or payment details from the information held by your mobile	**79%**
Alert your bank that you are roaming in a specific country so that you don't run into any problems with using debit or credit cards abroad	**75%**
Personalise ads based on your own personal information, under you control, rather than on the assumptions of major internet players	**65%**

In the interviews, the service providers were presented with various use cases for Mobile Connect. Both banks and governments were particularly interested in using Mobile Connect to check an individual's location (roaming verification). Banks were also very interested in using Mobile Connect to check various aspects of the customer's mobile account to counter fraud. Banks were also receptive to using Mobile Connect to enable a consumer to notify their bank when their phone is stolen or they have changed their SIM card.

89% STATED

They were interested in increasing the security of all their financial transactions.

Roaming verification
Mobile Connect can enable a consumer to share their location with their bank or a government agency that wants to check that they are abroad.

Banks and government agencies regard location as a particularly valuable attribute, according to the GSMA service provider research. Verifying roaming in this way can improve the consumer experience by enabling a bank, for example, to place fewer bars on usage, while reducing complaints handling and the need for a customer to inform a bank of their travel plans. In an interview, one service provider noted: "Nowadays, we trust mobile information more than financial information, because it is more likely that the customer has their mobile phone with them, than carrying a wallet."

Fraud scoring
Mobile Connect can enable a consumer to share or verify mobile account details with their bank or a government agency that wishes to check that they are who they claim to be. For banks and other providers of valuable services, the more information they have, the better their ability to detect fraud and reduce their risk exposure. "More [information] is definitely better," noted one interviewee in response to this use case.

Rather than using Mobile Connect to enable the consumer to give their explicit consent to each request for information, the service providers envisioned that Mobile Connect could be used to provide a straightforward opt-out mechanism or provide one-time explicit consent on registering Mobile Connect with the bank.

"Nowadays, we trust mobile information more than financial information, because it is more likely that the customer has their mobile phone with them, than carrying a wallet." **Service Provider**

5. Conclusions

Mobile Connect is well placed to address both service providers' and consumers' demands for straightforward and secure authentication and identification. The solution can help government agencies, banks and other service providers increase usage of their online services, improving efficiency, enriching the end-user experience and increasing engagement.

Assuming that the views of UK citizens are representative of those in other EU countries, Mobile Connect could be very widely adopted in Europe. In the consumer survey, 75% of the respondents said they would be likely to adopt Mobile Connect as their primary log-in for most websites, apps, and other online services. The GSMA's research found that consumers would feel comfortable using Mobile Connect in a wide variety of contexts and to access a broad range of services.

The specific challenges faced by banks and government agencies mean these sectors are likely to be among the lead adopters of Mobile Connect. In many scenarios, banks and government agencies are likely to use Mobile Connect to enable them to achieve the optimum balance between maintaining security, obtaining consent, and providing a smooth and straightforward end-user experience.

The findings of the research studies covered in this report suggest that Mobile Connect will increase usage of digital services by providing a simple and convenient authentication and identification solution. This will help the European Union to realise the objectives of the eIDAS Regulation and fuel the growth of Europe's digital economy.

Secure digital identity is now in our hands

Personal Data

GSMA Head Office
The Walbrook Building
25 Walbrook
London EC4N 8AF
gsma.com/mobileconnect
www.mobileconnect.io
Published: October 2015