mobile connect

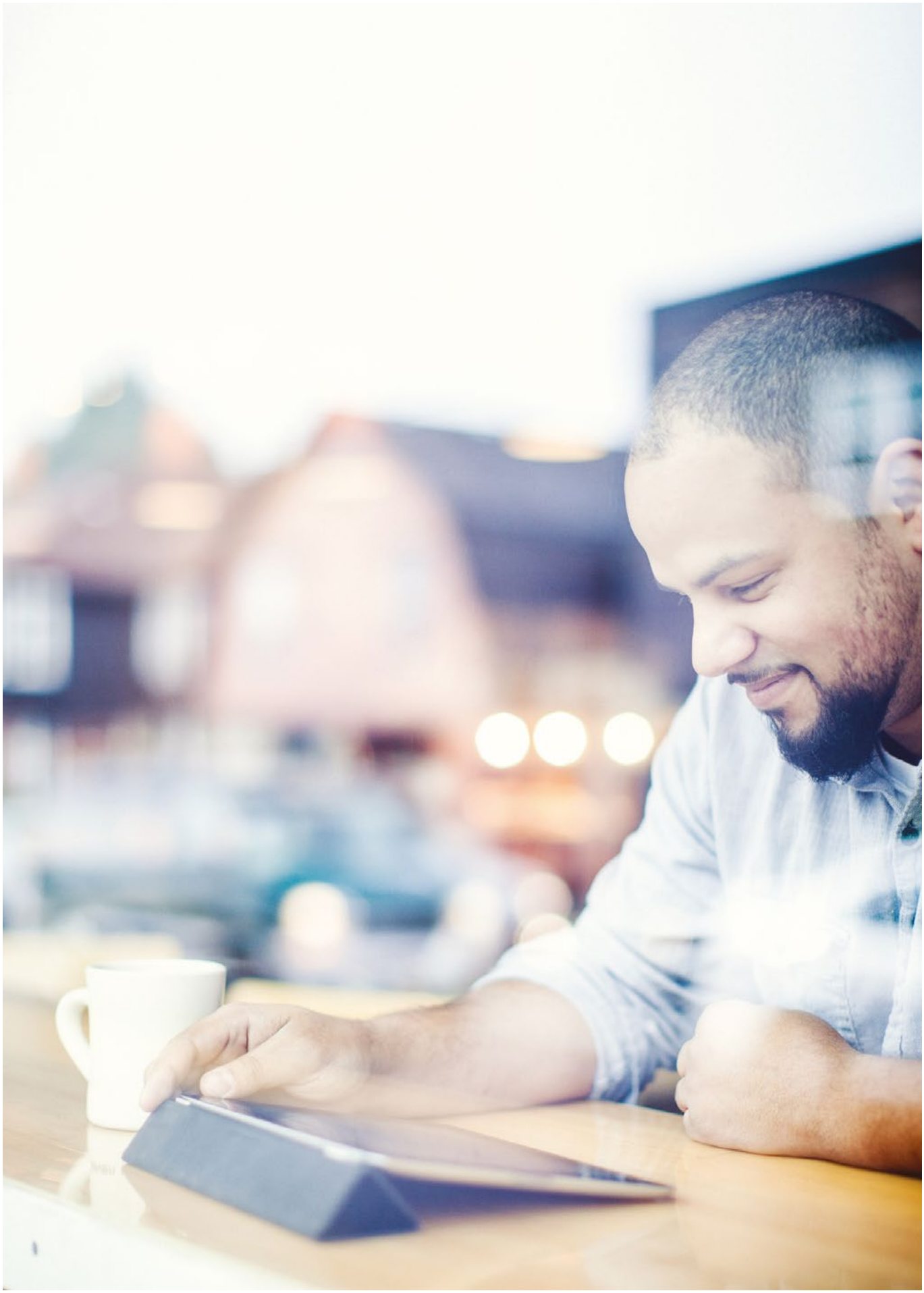
Mobile Connect: Mobile high-security authentication

Executive Summary

For consumers, digital services are convenient and cost-effective, but can mean compromising on their security and privacy. Developed by mobile operators, Mobile Connect makes it straightforward for users to authenticate, authorise or identify themselves securely, meaning they are less likely to abandon an online service. For example, when a consumer logs into an app or a website using Mobile Connect, they receive a message on their mobile handset, asking them to either confirm the action or enter a PIN in the case of more sensitive applications. No personal information is shared with the service provider without the individual's permission.

The key security benefits of Mobile Connect include:

- The use of "something I have", i.e. a mobile phone. as the primary authentication factor means Mobile Connect is less vulnerable to a scalable compromise/attack than the "something I know" approach used by password-based mechanisms.
- Mobile Connect requires the service provider and the application to be registered in advance. Before it can access the OpenID Connect Mobile Connect Profile, the service provider app is authenticated using pre-registered credentials. By checking whether the service provider is legitimate, this approach adds an extra layer of security.
- The Mobile Connect authentication system employs private and secure mobile network operator channels rather than the public Internet, meaning authentication is implemented through an entirely separate interface and mechanism. That prevents external entities from sending fraudulent messages or authentication prompts to the user. (Note: smartphone app authenticators use mobile data as a communication channel).
- Out of band authentication: with Mobile Connect, the consumer is authenticated via a different channel to the one through which they are trying to consume the service. In effect, Mobile Connect could be used to check that the user, the service access point and the authentication device are in the same place.
- Personal information, such as a phone number (MSISDN), is never shared with the service provider without the user's consent. Instead, a service provider-specific pseudonymous customer reference is shared. This token denotes a successful authentication and enables the service provider to identify the individual user. This approach means that the service provider doesn't know who the user is and service providers can't track a customer across different services. Mobile Connect works with the OpenID Connect standard, meaning all interactions are encrypted and the token is signed.
- Mobile Connect can support secure multi-factor authentication and authorisation, providing an appropriate level of assurance (LoA) authenticator, including multi-layer encryption, in line, for example, with the requirements of the EU Payment Services Directive.
- As well as harnessing the mobile device, the mobile network and operator's customer care capabilities, Mobile Connect could also employ contextual information captured by operators to help counter fraud and manage transaction risk.
- By establishing a single consistent approach globally, Mobile Connect enables mobile operators and service providers to benefit from economies of scale and interoperability, making security cost-effective and financially viable.



Introduction

Across all aspects of daily life, services are going digital. The convenience and cost benefits for users, service providers and society at large are both obvious and compelling. But many online digital services are not supported by effective identity, security and privacy capabilities, leading to user concerns and a growing trust deficit. Some 86% of users are concerned about security when online, according to a multinational survey commissioned by the GSMA.[1]

In the past, Internet security and privacy decisions have involved trade-offs. In the security domain, users typically have to sacrifice convenience for security or vice versa. In the privacy domain, free services are often funded through the commercialisation of personal information. As users generally have limited knowledge and understanding of these trade-offs, the resulting compromise might not represent a fair balance between user and service provider or be in the best interests of society. GSMA research[2] indicates that 81% of consumers don't feel that they are getting as much value from their personal data as third parties do.

Mobile operators can help to address the trust deficit by enabling users to use their mobile phones to easily and securely authenticate themselves and authorise digital services. Many operators are using the Mobile Connect solution for this purpose.

Through a single global interface, Mobile Connect supports authentication, authorisation, identity and attribute sharing or verification for service providers, whilst putting the user in control. Mobile Connect employs a combination of mobile device, mobile network and operator business process security features to enable the development of secure and user-friendly solutions for a wide range of online use cases including commerce and payments.

This non-technical paper is designed to address security questions related to authentication, especially with respect to payments, banking and online commerce. It explains how Mobile Connect can deliver improved security and privacy for consumers authenticating themselves online and authorising digital transactions, and how the solution will evolve in future.

1. Source: http://www.gsma.com/personaldata/wp-content/uploads/2015/09/Mobile-Connect-Factsheetv2.pdf
2. Source: http://www.gsma.com/personaldata/wp-content/uploads/2015/09/Mobile-Connect-Factsheetv2.pdf

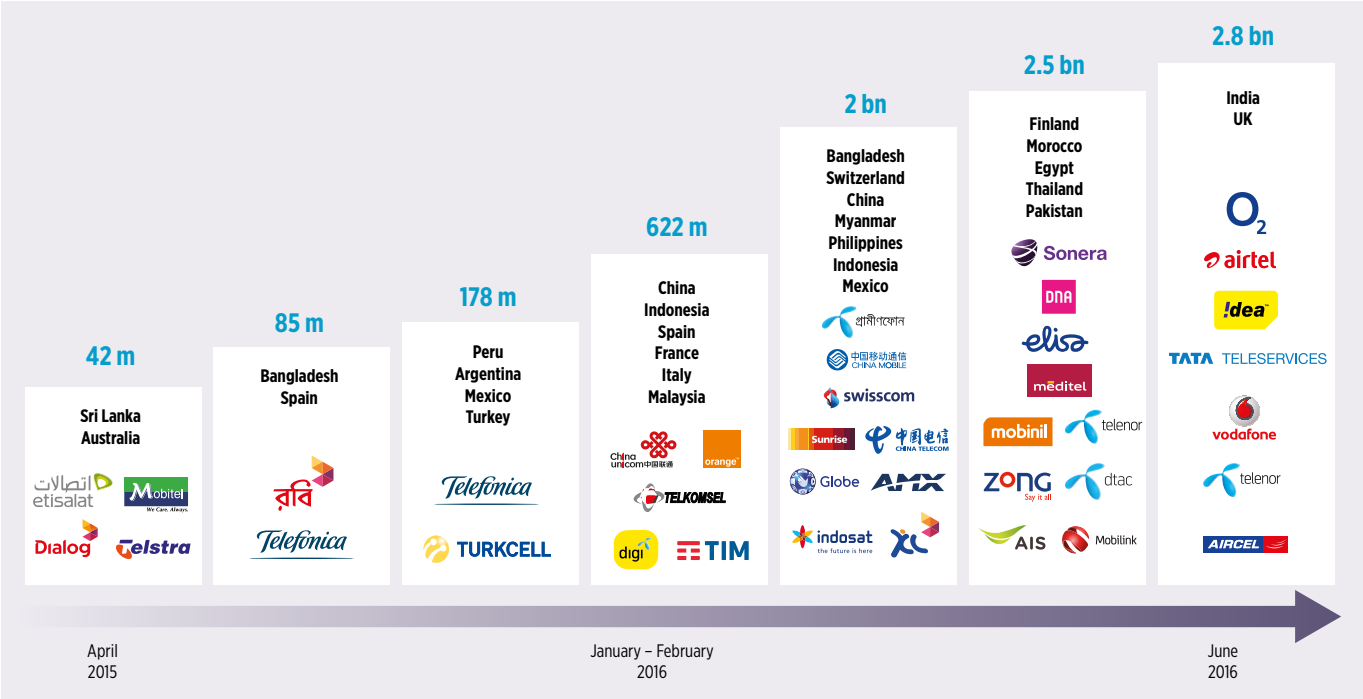
About Mobile Connect

By building security and privacy into digital services, Mobile Connect can help society realise the full benefits of such services. Provided by mobile operators, Mobile Connect is a global and federated solution for mobile phone-based authentication, authorisation, identity and attribute services. It can deliver appropriate security across many different use cases, including payment approval and public sector identification, without compromising user convenience or reach.

It enables users to interact conveniently and securely with service providers using their mobile phone, without the need to remember usernames and passwords for specific websites. At the same time, no personal information is shared with service providers without the user's permission. Mobile Connect can support online services consumed from any device, but the mobile handset is always the authentication device.

For service providers, Mobile Connect can increase user engagement by improving security and reducing friction. Moreover, it can now reach 2.8 billion Mobile Connect-enabled users globally (see graphic). It also benefits from being provided by well-known and trusted mobile operators with a physical presence in the markets where consumers live and work.

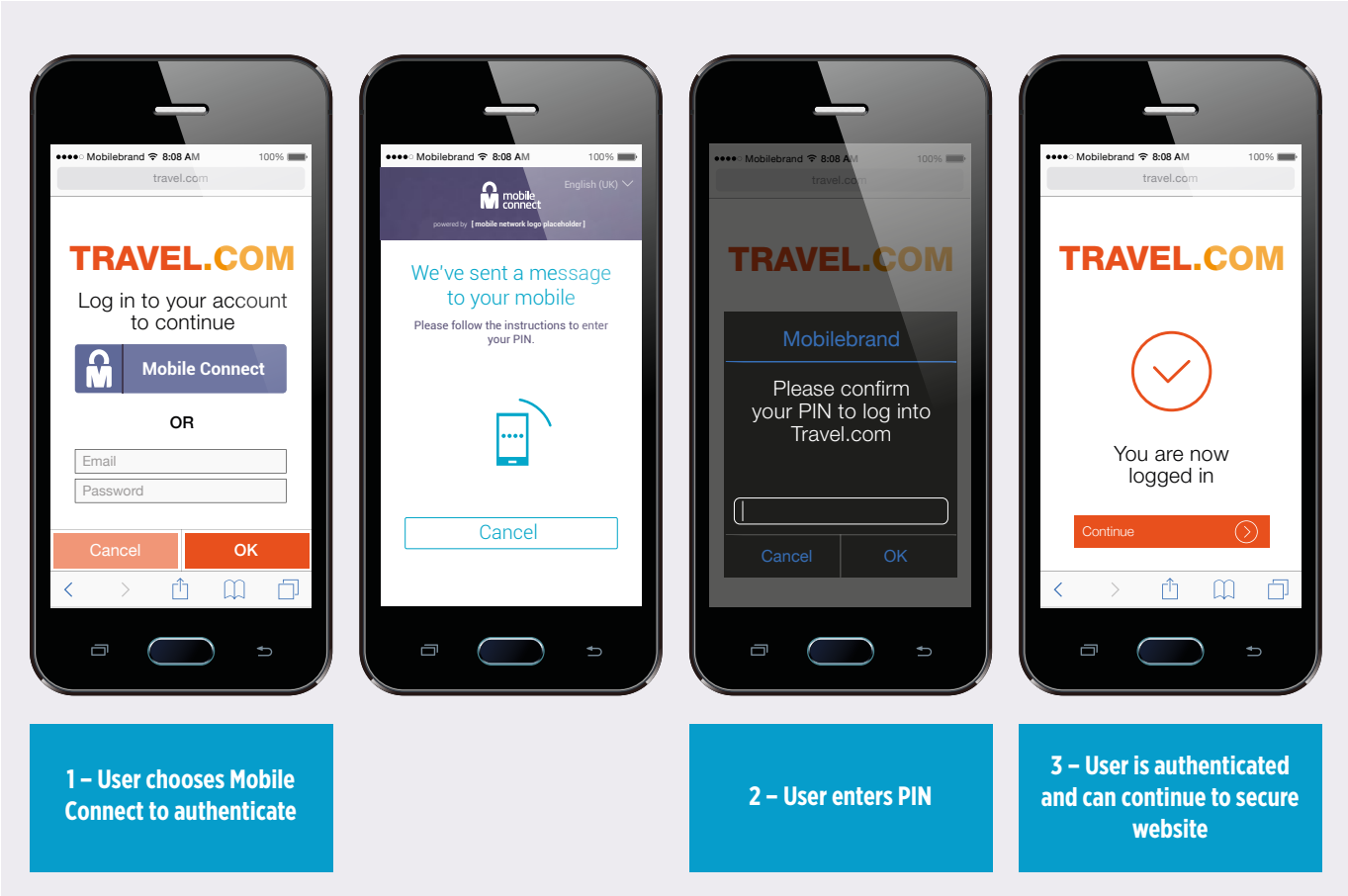
Global growth of Mobile Connect (enabled users)



How it works – straightforward yet secure

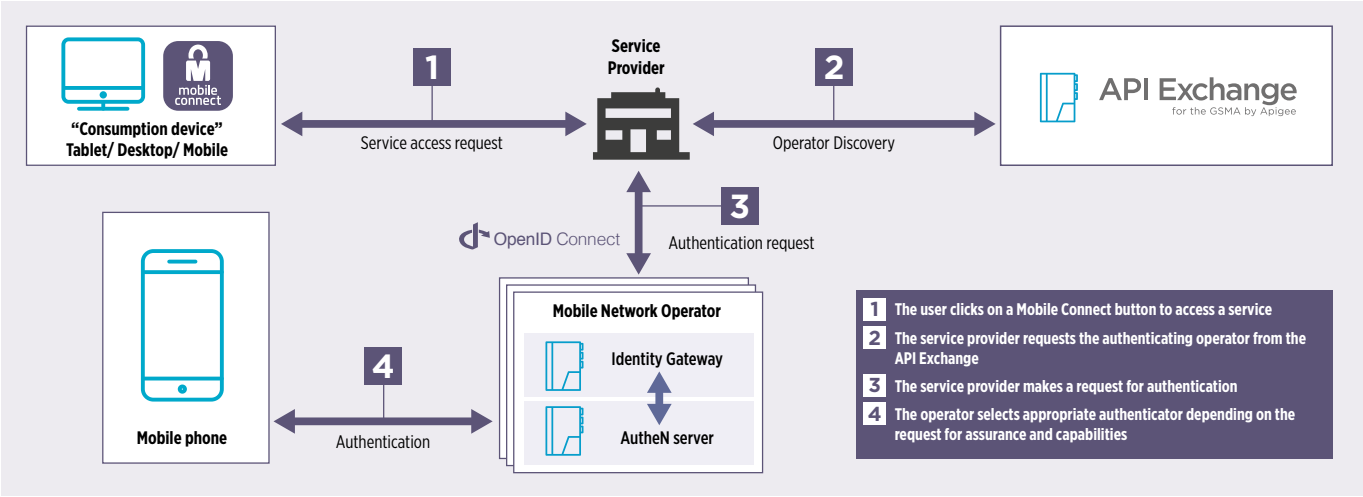
Mobile Connect applies the same simple core user experience regardless of the mobile network operator, the service provider or the operating system used by the handset. On a new website or app, the user clicks "Log in with Mobile Connect". They will then be asked to enter their mobile number into the pop-up window. The mobile number is not shared with the website or app. Instead, the mobile number is used by the API Exchange, provided by GSMA, to discover the user's mobile operator. The online service or app can then make the request directly to the operator. The operator then uses SMS or the USSD channel - or mobile data in the case of smartphone app authenticators - to send a prompt to the user's phone to either press a button or provide a PIN (see graphic). In this way, Mobile Connect can combine the user's mobile device associated with a unique mobile number via the SIM ('something I have') and PIN ('something I know') to verify and authenticate the user. As an alternative to a PIN, the biometrics capability intrinsic to many smartphones, such as a fingerprint ('something I am'), could be used as the second authentication factor. Upon successful authentication, the user is logged in anonymously without sharing any data with the website or app.

In this way, Mobile Connect supports high-security two-factor authentication, while alleviating consumers' privacy concerns and increasing the likelihood that they will engage with a specific service. For less sensitive applications, this process can be simplified further so that it isn't necessary to enter a PIN. For more information about different levels of authentication, see question 4 in the Q&A.



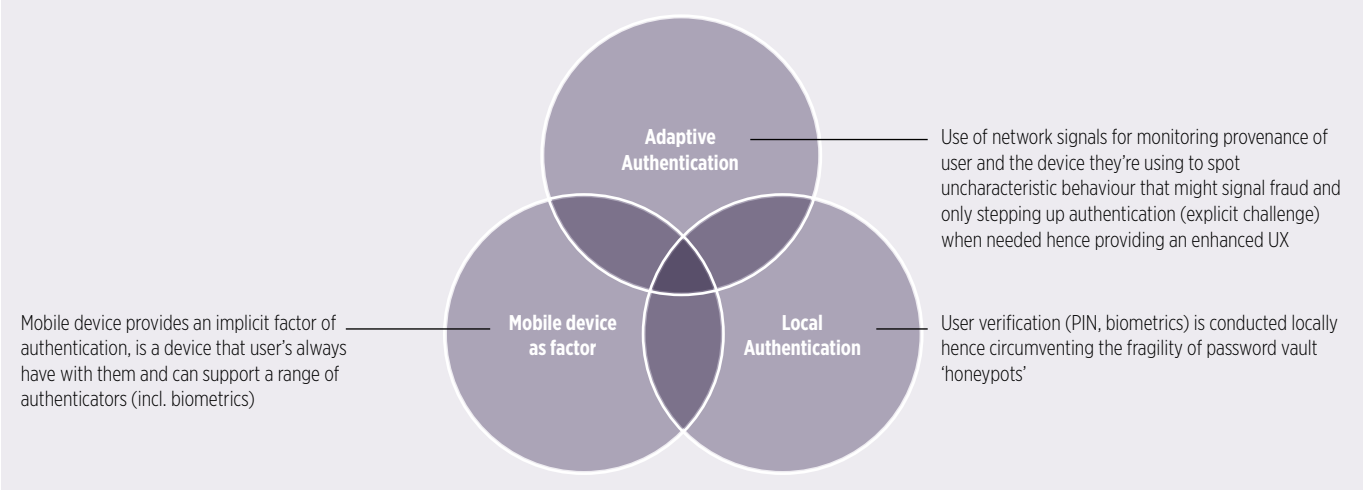
A standards-based solution

Mobile Connect is built on OpenID Connect; a widely-used open standard, which can be delivered either by open source platforms, making it simple and cost effective, or with bespoke platforms. OpenID Connect is used to exchange an authentication token between the mobile operator and the service provider (see graphic), ensuring secure communication for both consumers and service providers.



Security and privacy dimensions of Mobile Connect

With the permission of users and appropriate privacy safeguards, Mobile Connect could be used to combine the security of the mobile device, the mobile network and operator business processes with contextual network information (see graphic). All these dimensions can complement and enhance each other. Even if security is breached in one dimension, this is discovered and mitigated by the other complementary dimensions. This approach could deliver appropriate security across all use-cases, including payment approval and public sector identification, without compromising user convenience, privacy or reach.



The Role of the Mobile Device

Many consumers rely heavily on their mobile devices. In many developed markets, smartphones are becoming indispensible. For example, on an average day, 39 per cent of millennials (people aged 18-34) in the US interact with their smartphone more than anything or anyone else, according to a study by the Bank of America[3]. For the population as a whole, that figure is 29 per cent. In general, consumers are highly aware of their mobile device, keeping it close to them and have little tolerance for other people using it. The Bank of America survey found that 29 per cent of respondents feel anxious when they don't have access to their smartphone, rising to 39 per cent among millennials. If they can use their mobile phone to authenticate into different services in a familiar way, consumers are more likely to feel secure.

The following aspects of the mobile device are employed by Mobile Connect security:

Mobile Connect requires the user to have physical access to their mobile device. When accessing a website, for example, the customer receives a pop-up message on their registered mobile device to access the website[4]. Depending on the security level, the customer may have to also enter a Mobile Connect PIN via the mobile device.

Mobile Connect's distributed architecture is more robust than centralised solutions. Mobile Connect's use of a physical authentication factor (the mobile phone) makes it more secure than most existing online authentication solutions, which often rely entirely on digital/knowledge methods, such as entering a user name and password on a website. Purely digital authentication mechanisms can be hacked in large numbers by breaking into the central database, while authentication using 'something I have' as a pre-requisite makes any fraud attack less scalable. To mount an attack at scale, the attacker would need physical access to large numbers of mobile phones. A physical mobile phone linked to a phone number cannot easily be cloned. Moreover, Mobile Connect uses out-of-band authentication - authentication is conducted via the mobile device irrespective of the medium through which the service is consumed. For more information on out of band authentication, see question 3 in the Q&A.

Mobile Connect does not store any sensitive data (e.g. PIN, token) on the physical mobile phone. The hash of the PIN is stored in the SIM applet and, for USSD, the hash of the PIN is stored in the secure servers of the mobile operators. None of the secure credentials are ever shared with the service provider, which receives a specific pseudonymous token instead. For more information on the handling of credentials, see question 2 in the Q&A.

A TEE (Trusted Execution Environment) provides a secure, tamper-proof execution environment at the hardware level for applications. Mobile Connect recommends that applications use a TEE on the device whenever possible.

The mobile device is authenticated into the mobile network via the SIM. By representing the mobile network within the mobile device, the SIM ensures a secure two-way connection between the mobile device and mobile network.

The Role of the Mobile Network

Secure by design, a mobile network can disable a device's SIM card and flag the device as lost or stolen in a global database. For more information on this process, see question 1 in the Q&A.

The subscriber's mobile network knows which device is connected to which SIM and MSISDN (telephone number). It uses mutual authentication mechanisms to establish trust: a device (represented by the SIM) is securely authenticated by the mobile network and at the same time the device (represented by the SIM) authenticates the mobile network. If either the device or SIM is exchanged for another, the mobile operator could flag this behaviour to user-approved service providers and potentially even block the SIM if there is cause to believe the device has been stolen.

3. Source: http://newsroom.bankofamerica.com/press-releases/consumer-banking/fess-majority-americans-deny-their-smartphone-behaviors

4. In cases where the consumer has no device at hand because the battery is flat for example, the consumer could fall back to logging-in via the traditional way by entering the username and password, instead of using Mobile Connect.

The mobile operator could enhance the security of the overall mobile ecosystem by utilising contextual information available in its network. Below are some examples of contextual information that can enhance security:

- **Is the device (represented by the SIM) in its usual location?**
- **Has the SIM been changed frequently (abnormal behaviour)?**
- **Has the device been changed frequently (abnormal behaviour)?**
- **Is the user a contract customer user (enhances confidence)?**
- **How long has the user been a customer of the mobile network (enhances confidence)?**
- **Is the device (represented by the SIM) roaming at the moment?**

The Role of Business Processes

Mobile operators' typical business processes ensure that the user has a way to report events, such as lost/stolen devices or an account compromise/takeover. Depending on the situation, the appropriate action can be undertaken by the mobile operator via established customer care processes, i.e. disabling/enabling the handset and/or SIM remotely. As an operator has a billing relationship with its subscribers, it already has account management and dispute resolution processes with its customers in place.

A mobile operator could design their business processes to react to abnormal behaviour, such as a change of SIM or handset, in cases where there is already a suspicion of fraud or a lost/stolen phone or some other concern regarding the security of the transaction.

Open ID Connect platform: secure interfaces within the ecosystem

Open ID Connect provides secure interfaces between Mobile Connect infrastructure and service providers. A widely-used standard, OpenID Connect is simple and cost-effective. It has already been adopted by key players, such as Microsoft, Google and Salesforce.com. Standardisation reduces key entry barriers enabling smaller companies to offer services.

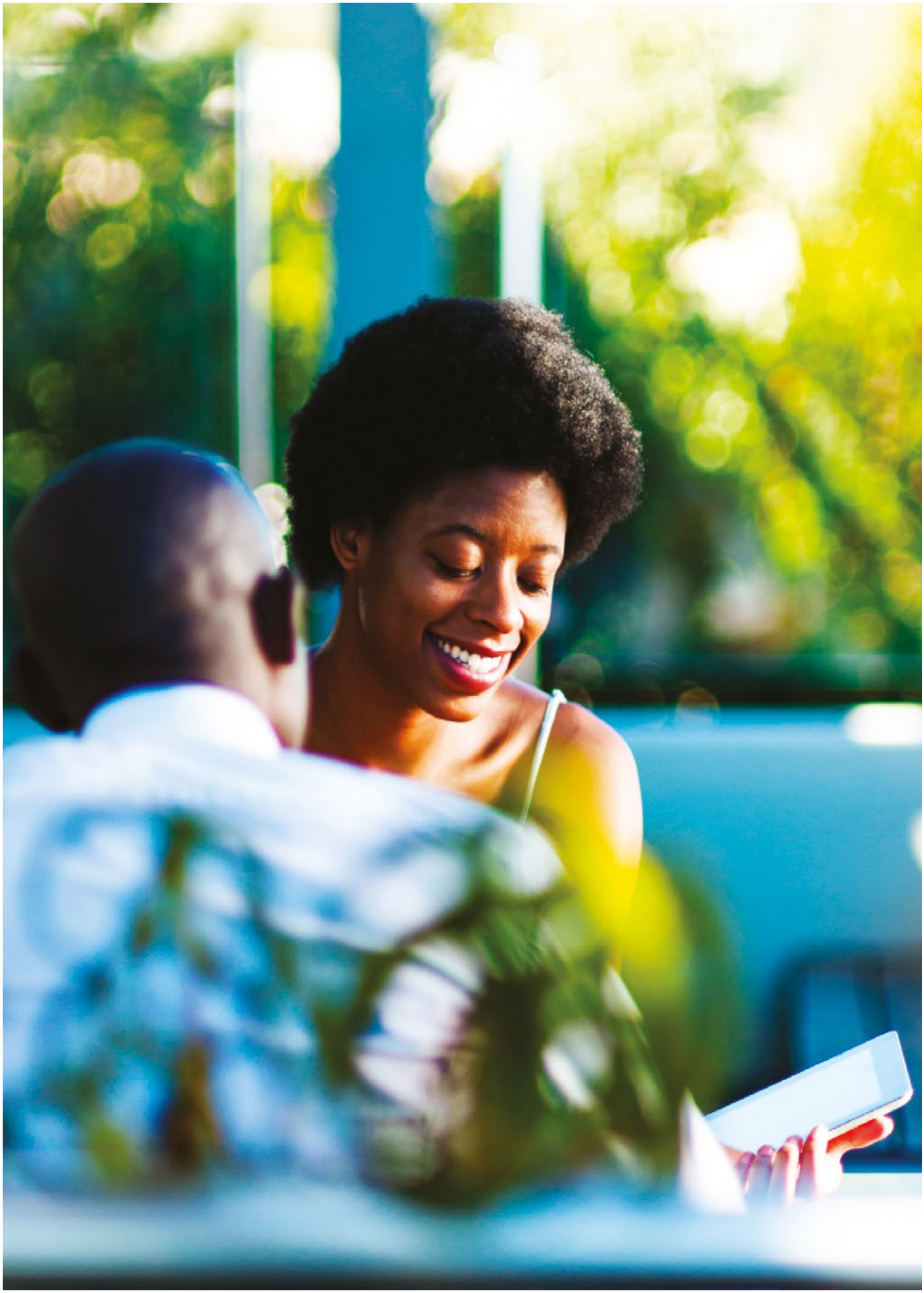
The global consistency of application programming interfaces (APIs) across operators is a key part of the Mobile Connect value proposition. Only one technical integration is needed in order to reach any Mobile Connect user regardless of which mobile network they use. This cost-efficiency and scalability is an important aspect of a viable security solution.

Open ID Connect not only authenticates the user, but also the service providers. Service providers are assigned client credentials when they register to use Mobile Connect. Only service providers with the correct client credentials, which are used to authenticate transactions, can participate in Mobile Connect. This helps create a framework of trust between participating organisations.
With OpenID Connect, tokens are exchanged between Mobile Connect and service providers. Tokens are specific to the service provider (each user has a different token for every service). This protects the customer from being tracked across different service providers, increasing privacy for the user. To provide message integrity, the messages are signed by the Mobile Connect provider, (i.e. the mobile operator) for non-repudiation.

Mobile Connect Privacy

Mobile Connect is governed by a set of privacy principles that apply to the processing of personal information by operators and third party service providers. The 'user-centred' principles are based on a common understanding that those who design, implement and operate identity services are committed to ensuring good privacy and security practices that respect and protect the privacy of individuals and the security of their data[5]. One of the core principles is it that user information that is shared with third parties should be proportionate to the purpose and must only be shared based on user permission. For example, to buy age-restricted goods, the date of birth does not need to be shared, just information on whether the user is older than a certain age or not.

5. Link to Mobile Connect Privacy Principles



Q&A on Security

What happens when the mobile device is lost/stolen?

The user calls the operator's customer care service and reports the phone lost or stolen. The operator in turn blocks the SIM from usage and the device ID [IMEI] can be marked in a cross-network equipment register as a stolen device. This is then propagated to all mobile operators globally with access to the equipment register database.

Even when a handset is lost or stolen, the operator has the ability to disable the SIM in the device over the air.

How are consumers' personal security credentials (i.e. the Mobile Connect PIN) protected?

User security credentials are treated as "personal", meaning they are never shared with a third party. User security credentials have the following characteristics:

- **Creation: The user creates the security credential and user verification (the PIN or biometrics) locally hence circumventing the fragility of password vault 'honeypots'.**
- **Storage: Credentials are always hashed before being stored. The storage location is dependent on the authenticator being used. Where the authenticator is the SIM applet, hashed credentials are only ever stored on the SIM. Where the authenticator is USSD-based, hashed credentials are stored securely on the Mobile Connect secure server.**
- **Transportation: Credentials are transported using secure channels, e.g. using encrypted messages or mobile network signalling channels.**

How does out-of-band authentication improve the security?

Out-of-band authentication refers to the use of separate devices or channels for "consuming" the service and authentication for service access. For example, the user can consume the service in a Wi-Fi connected tablet, laptop, smartphone or a smart TV and get authenticated using their mobile phone via the SMS or USSD channel of the mobile network.

The explicit separation of the two devices and/or channels – the consumption device/channel and the authentication device/channel - introduces multiple points of integration – separated by different access controls. For example, the service consumption device is accessed directly by the user and the service provider, but the authentication device is accessed by the operator and the user in a secure mobile network environment.

Any security attack would need access to both devices or channels at the same time and also needs access to both the separate sessions (in the consumption device and the authentication device), which adds practical barriers to a security attack, and makes it less scalable for the attacker.

Is there much difference in the level of security between LoA3 and LoA4 Mobile Connect solutions?

Mobile Connect uses the standard Level of Assurance (LoA) definitions from ISO 29115 for authentication: a global standards-based approach to authentication security. LoA3 is a high-security two-factor authentication solution. LoA4 requires, in addition to LoA3, that the security credentials are based on PKI technology. In practice, LoA3 is comparable to European eIDAS directive defined security level "substantial" and LoA4 is comparable to "high".

Within the Mobile Connect framework, LoA3 service is typically achieved using a SIM applet with security credentials placed on the user's mobile phone SIM secure element, together with strong encryption for messages to and from the SIM. For LoA4, the SIM applet has PKI security credentials. There is a theoretical difference in security between normal (symmetric) and PKI credentials (asymmetric), but in practical day-to-day use, the difference is negligible. In fact, the use of additional security features, such as mobile operator business processes and dynamic mobile network data, may be more effective in increasing overall security and fraud resistance than by the addition of PKI certificates.

Both LoA3 and LoA4 Mobile Connect implementations are suitable for the vast majority of public and private sector high-security use cases, especially when combined with additional security features. The primary exception is digital signature services, where non-repudiation requires the use of PKI credentials.

What are the main benefits of Mobile Connect compared to other widely used two-factor authentication solutions?

Most common two-factor authentication solutions in use today are one-time-password delivered via SMS (SMS-OTP) or through some other means, authentication hardware tokens (smartcard or "USB-dongle") and increasingly also biometric solutions (fingerprint, iris or facial scan). In addition to these, there are new solutions introduced at a rapid phase but typically they still lack scale among users.

Mobile Connect uses the mobile phone as the "something I have" factor in the two-factor authentication. For users this is convenient, as they tend to have their mobile phone always within immediate reach and it eliminates the need to carry something extra just for authentication purposes. Also secure storage and use of multiple hardware tokens for different services has proven challenging – not to mention the often high cost for service providers of supplying the tokens for all users.

In comparison to one-time-password solutions, Mobile Connect offers better user experience as there is no need to copy the code from one medium into the other. This reduces time and errors in authentication – while at the same time improving the security against many attack vectors.

Biometric solutions can well be used within Mobile Connect as authenticators. Biometric authenticators have both benefits as well as weaknesses compared to other alternatives. On the benefit side, most commonly cited are ease-of-use and security.

Conclusions

Mobile Connect provides a consistent, straightforward and secure mechanism through which online service providers can authenticate users. It can also be used to enable consumers and service providers to exchange specific attributes, such as location, in a secure and straightforward way that enables the individual to maintain control over their privacy. By harnessing the capabilities of the mobile network, the mobile device, operators' business processes and contextual information, Mobile Connect offers a much higher level of assurance than password-based authentication mechanisms implemented over the public Internet.

By combining ease-of-use with robust security and privacy safeguards, Mobile Connect encourages consumers to interact and engage with service providers, helping both parties realise the full benefits of digital services. With the arrival of Mobile Connect, consumers and service providers no longer need to compromise on convenience or security.

Floor 2, The Walbrook Building
25 Walbrook, London EC4N 8AF UK
Tel: +44 (0)207 356 0600

mobileconnect@gsma.com
www.gsma.com/mobileconnect