Deloitte.

Telco's mobile based digital authentication and identity in digital ecosystem and economy

Introduction

An estimated 650 million people will be online in India by 2020, with mobile phone as primary device for access. Today, c. 60% of the search queries and 70% of e-commerce transactions take the mobile phone route. By 2020 c 25% of India's population would have shopped online at least once.

To benefit from this burgeoning mobile based digital ecosystem, many digital merchants[1] are adopting or transitioning to *'Mobile First'* or *'Mobile Only'* strategy. The increased online usage and transactions has outgrown traditional username-password combinations, making it a struggle for users to remember all of their different login credentials.

As a result, two major issues came to the forefront: first, security risks and inconvenience for users and second, rise in abandoned transactions and service delivery risks for digital merchants.

Future of traditional logins and passwords

According to a GSMA study[2], 40% of users forgot password once in a month and 86% of users leave a website when prompted to register. The poor user experience of current password retrieval methods is forcing new, unique and captive users to leave the websites prematurely leading to rise in abandoned transactions resulting in loss of revenue for digital merchants.

Analyzing the above issue, digital merchants and the start-up community fully recognize, the need for user security transformation in terms of authentication, identity and authorization methods as these are the major control points in the digital economy. It is also considered that the security transformation should not compromise user experience in terms of simplicity, seamlessness and convenience - whether buying a product from an ecommerce portal, booking a flight ticket, doing a banking transaction or paying utility bills etc.

1. Digital merchants are online service providers who leverage on digital technologies for customer acquisition and engagement by providing end-to-end digital experience.
2. Based on GSMA Consumer Research Report (2015)
3. OTP involves sending a temporary authentication code via SMS to the user's mobile phone based on the mobile number that is initially provided at the time of signup/registration

In the subsequent sections, we discuss the shortcomings of current user authentication practices and analyze how the security transformation is shaping up with respect to new authentication methods.

One Time Password

Today, One Time Password (OTP[3]) is in vogue. This approach is fine to verify the user when an application is installed or a particular service is requested for the first time. Asking the user repeatedly to enter an OTP for every subsequent transaction can be vexatious experience as the user has to leave the application, retrieve the OTP, key in and submit it.

Due to lack of a better alternative, many digital merchants are using auto OTP reader method to improve user experience (the OTP auto reader submits the code itself into the application on behalf of the user). With growing privacy concerns, many users frown upon this method. In addition, there is no guarantee this will work always and many a time, users are forced to leave the application to retrieve the OTP from their SMS inbox - resulting in a fragmented and inconsistent user experience.

Transformation of user authentication

Based on the insights gained above, the need for more secure, seamless and convenient digital authentication methods is reasonably established. But how this will be provided and who will play a role in the ecosystem of next generation digital authentication methods? Until now, no one has owned the user authentication space conclusively except a few nimble start-ups who have come up with some innovative ideas. But one thing common in majority of the authentication solutions is use of mobile number (MSISDN) as the Identifier, which uniquely identifies the user. From the individual user's perspective, mobile number is more personal than any other attribute. Given this, can mobile operators (owner of SIM card information) collaborate with digital merchants in this area?

Well the answer is that mobile operators have a real opportunity and blueprint to play a pivotal role in providing the next generation authentication solutions – that is not only strategic but also relevant in the overall digital ecosystem. To initiate this, the mobile operators and digital merchants can leverage on the GSMA Mobile Connect Initiative, which is part of the larger GSMA personal data program.

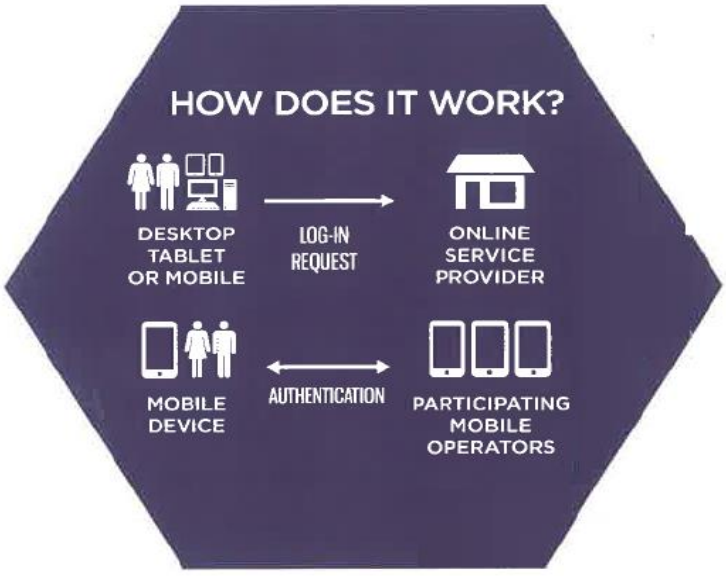
GSMA Mobile Connect

GSMA Mobile Connect is a new, simple and convenient solution providing users with universal secure & privacy-centric authentication services, facilitated by mobile operators leveraging on their

inherent security of mobile networks and SIM. It is designed to position mobile operators as trusted providers of – Authentication, Identity and Attribute brokerage services.

Authentication is basically challenging the user to prove *'who you are based on who you claim to be'*. It is for the digital merchants to do the verification by asking user credentials that corroborate the claim. To address the growing issue of abandoned transactions, digital merchants are in need of applying varying degrees of user authentication methods (simple to strong) based on the privacy and level of service request. Let's understand from both user and digital merchant's perspective the working of mobile connect.

How Mobile Connect works?



Source: GSMA

As shown in the above flow diagram, Mobile Connect allows users to quickly authenticate their identity to third party digital merchants (example: ecommerce, banking, government portals etc.) without the need for users to disclose their mobile number, create or remember logins and passwords. To protect the user identity, instead of mobile number only a token in the form of a Pseudonymous Customer Reference (PCR) is passed to the digital merchant – this achieves the user privacy objectives while ensuring the authenticity of the user.

This basic flow is similar for all - from simple to strong authentication methods. In all Mobile Connect supported authentication methods, the authentication device is always the user mobile phone (*'demonstrates something I have'*) while the consumption can be on any device. When the user opens the website or portal on any consumption device - feature phones, tablets, smartphones, and desktops or laptops, the request for authentication is initiated by user by clicking on the 'Mobile

Connect' logo, which is then received by the user's serving mobile operator. The mobile operator authenticates the user by mapping the PCR token received from digital merchant against user's mobile number & other SIM parameters and provides the confirmation back to the digital merchant.

Mobile Connect supports simple to strong authentication methods

SIMPLE/SINGLE FACTOR – CLICK OK	**Something I Have**
	Simple/Seamless Authentication
	Used to enable larger user base

TWO FACTOR – PIN based	**Something I Have and Something I Know**
	Higher level of security with PIN
	May be applied for premium services

STRONG AUTHENTICATION – PIN + Encryption (PKI)	**Something I Have and Something I Know**
	Very Higher level - Crypto SIM and applet based
	May be applied for high value transactions

As shown above, single factor authentication is simple and can be seamlessly used for mobile number verification instead of OTP. Two factor authentication, which is more secure, challenges the user to enter PIN. This PIN is created by the user during the one-time Mobile Connect registration. The same PIN ('*demonstrates something I know*') can be used by the user at any digital merchant website/application, which supports Mobile Connect as an authentication option. With this universal PIN, the issue of multiple passwords can be addressed to the comfort of user, subsequently benefitting the digital merchants with increased transactions.

Mobile Connect also provides much stronger authentication methods, which uses both PIN + PKI based encryption. PKI is a highly-secure method based on two types of keys: public keys, which are freely accessible to all, and private keys, which the user (and only the user) stores a local copy of.

The PKI allows user to encrypt PIN with their private key that is stored on their SIM card. This method is useful in high value financial transactions, particularly involving the banking sector.

Combining Mobile Connect and user attributes provided by mobile operator

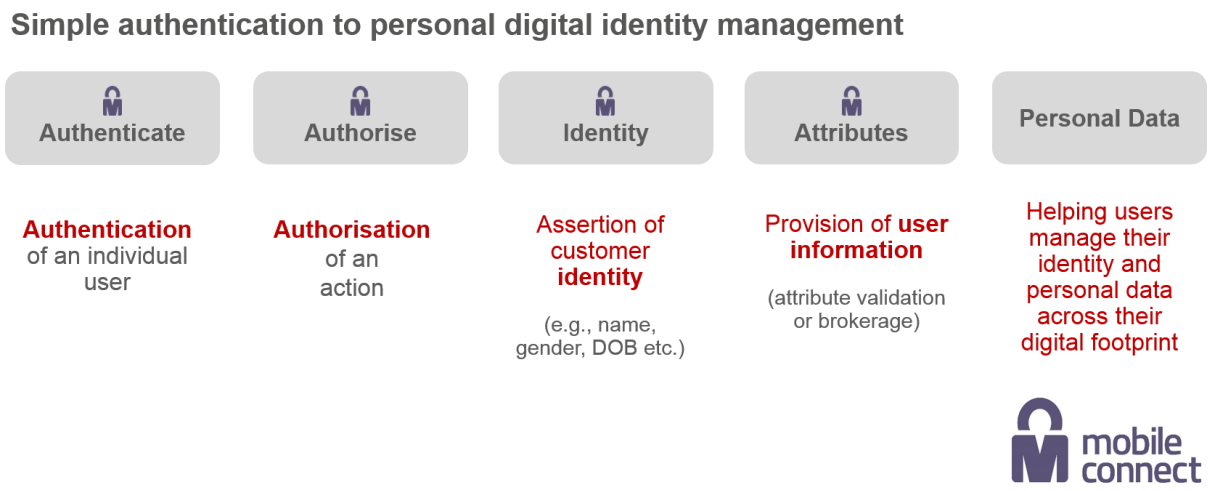
In addition to providing above compelling authentication methods, there is more that Mobile Connect can do. Mobile operators can provide other user attributes like location, demographics, age, account type (post or prepaid), mobile device type & model and network usage information, and in doing so, deliver a new authentication factor: *'demonstrates something the network knows'*. Digital merchants can gain access to these user attributes to provide a continuous and enhanced personalized service experience. Attributes are provided only after obtaining user's permissions in line with the applicable privacy policy. An important principle of Mobile Connect is that only user information is shared. So for instance, when verifying the user age is over 18 years old, only True/False is returned instead of actual DOB.

Attributes and Identity are closely related concepts. Some of these user attributes can be used by digital merchants to address the challenge of establishing absolute digital identity of the user either by combining all or a set of them. The attribute framework that is being put in place by GSMA and mobile operators will facilitate wide range of use cases cutting across industry segments, like ecommerce, travel industry, healthcare care, government services etc (KYC validation, age verification, roaming checks etc.)

Mobile Connect deployment approach

Initially, digital merchants can deploy Mobile Connect for simple authentication of individual by verifying user on '*who you are based on who you claim to be'* and proceed to authorization, which is the process of verifying that *'what you are permitted to do based on what you are trying to do'*. Therefore, authorization entails authentication. Identity assertion and attribute sharing depends on mobile operator capabilities to share customer information.

(Note: Simple authentication is not mandatory to the deployment of other product areas).



Source GSMA

Status of Mobile Connect deployments globally and in India

Following successful trials and development of the authentication proposition with a lead group of operators during 2014, Mobile Connect is now beginning to go live: March 2015 saw the official launch of Mobile Connect by 42 operators in 23 countries, with others committed to launch during the remainder of 2016.

The good news is that in 2015, all major Indian mobile operators and GSMA formed a multi-operator Mobile Connect industry consortium to work on the Mobile Connect launch plans. Based on the information available all Indian operators have launched Mobile connect in India on 19th July 2016. They are already working with a few digital merchants in the ecommerce & travel space and are also in advanced discussions with leading banks to integrate Mobile Connect. The Mobile Connect deployment can be expanded in a number of directions by the mobile operator based on their own capabilities and digital merchant's needs. Some of the Mobile Connect use cases that will help digital merchants are:

1. Single factor zero-knowledge mobile number verification for banks replacing the SMS OTP
2. Mobile number verification to seamlessly verify customer mobile number replacing SMS OTP
3. Identifying actual user app installations against fake ones with seamless user device verification

Next steps with Mobile Connect

The immediate priority for both mobile operators and GSMA is to onboard more digital merchants across all verticals and help them integrate with Mobile Connect. To expedite the Mobile Connect uptake, there is a need to create powerful engagement and outreach programs involving other digital industry stakeholders, all helping towards building a vibrant and sustainable mobile based digital security ecosystem.

Mobile Connect as core framework offers a tremendous opportunity to digital merchants to address their current user authentication and identity challenges as discussed above. By critically assessing the digital merchant's immediate authentication needs across all sectors and collaboratively working with mobile operators, GSMA and other stakeholders, new milestones can be reached.

Neeraj Jain

Partner, Consulting – Strategy & Operations

Deloitte India

psayini@deloitte.com

Prakash Sayini

Director, Consulting – Strategy & Operations

Deloitte India

psayini@deloitte.com