GSMA Mobile Identity

Dialog Connect:

A Case Study

Written by the Mobile Identity Team

Contents

I Introduction

Identity in Today's Growing Digital Economy

As the global market for online commerce, social media, gaming and other activity continues to expand rapidly, the need to accurately authenticate the identity of individuals and organisations for access and use of these services has grown significantly. Whereas in the real world, identity can be verified through the use of physical tokens, such as ID cards, passports and other documents – supplemented by face-to-face interaction – in the digital world, the process of establishing that an individual is who he or she claims to be is materially more complex.

In the realm of ecommerce, in which nearly $1 trillion of business is transacted globally, the vast majority of buyers and sellers have never met, and never will. Yet the identity assertion processes used in the online world are often remarkably weak: in most cases, the individual creates their own identity credentials – a username and password – and the service provider can do little to verify the identity of the individual to which they pertain.

As a result, the digital identity that each individual creates is inherently insecure (because the only credentials are a username and password that the individual self-selects) and need not relate to a real human being (individuals, and indeed criminals or computers, can create artificial identities, often for the purposes of perpetrating fraud). Consequently, these identities typically fall short of the requirements of higher-risk, higher-value use cases such as online shopping or accessing e-government services.

Dialog Connect: Resolving the Identity Challenge in the Emerging Market Context

These challenges pertain just as much to emerging markets, where internet penetration is growing at a rapid pace, as they do to markets where online activity is part of daily life. In Sri Lanka, as elsewhere in the world, there are many internet-based identity providers. However, all of these entities lack the ability to resolve a digital identity to an actual person.

With this in mind, Dialog's Connect service is designed to deliver a strong authentication process in support of these and other use cases. Leveraging the same registration process that is required to take a mobile subscription in the first place, Dialog subscribers are required to attend one of the company's retail stores, and present their identity card and a contemporary utility bill or bank statement (proof of address), in order to verify their identity. Once appropriate checks have been made, Dialog can then create a digital identity, bound to that registration process, which suffers none of the risks that arise in online self-registration. A PIN code is sent to the subscriber's mobile, and that PIN is introduced to Dialog's online portal, to finalise the process of establishing a Connect identity. Once created, that identity can be used to access content and services, and even undertake transactions, via a wide range of third party partners.

Dialog Connect is effectively a form of federated identity: the identity of any given individual can be used to access to the goods, services and content and of any and all federated third parties (service providers). The benefits to subscribers are many. The most important is security; the Connect identity is created on the basis of a robust and rigorous registration process, and creates a unique and secure digital identity, which can only be accessed by the subscriber.

Additionally, this federated approach relieves subscribers of login fatigue, by allowing a single identity to access multiple third parties (as opposed to the subscriber having to create a username and password for each one). The single-sign-on capability further reduces this common frustration by removing the need for the user to re-authenticate on partner sites. Future linkages will allow the solution to also make payments easier: rather than having to provide bank or credit card details to each service provider, Dialog Connect will soon allow the cost of purchases to be added to the subscriber's mobile phone bill using Dialog'sAdd2Bill service which is already in operation.

As a result, the benefits to participating service providers are similarly clear. Since only a minority of the population of Sri Lanka use credit cards (just over 50% of the population have bank accounts, while approximately 600,000 people have active credit cards), the capacity to add purchases to a mobile phone bill is of material value (not least because the vast majority of the Sri Lankan adult population are mobile subscribers). Importantly, the Dialog Connect service is available to subscribers of other mobile networks, meaning that participating third party service providers can address, in essence, the entire adult population of the country via a single, integrated platform.

Leveraging the SIM: A New Role for Mobile Operators

From the perspective of Dialog itself, and the other mobile operators in Sri Lanka, the list of benefits is also substantial. At a strategic level, the Connect service positions the SIM card at the heart of authentication spanning use cases way beyond those normally associated with mobile phone usage; in short, it establishes the SIM card and the mobile medium as a frontline identity management service provider. More materially, the service allows mobile operators – Dialog most particularly – to participate in the critically important e-commerce market, from which operators have historically been excluded (or at least marginalised).

In time, operators will be able to derive substantial revenues from their presence in this critical, and fast-growing market. More broadly, and as illustrated below, the Connect service helps to extend the reach and presence of operators' brands, such that their profile is raised, levels of awareness are increased, and ultimately, loyalty is manifest.

Operator Profile

Dialog: Leading Innovation in the Sri Lankan Mobile Telecommunications Sector

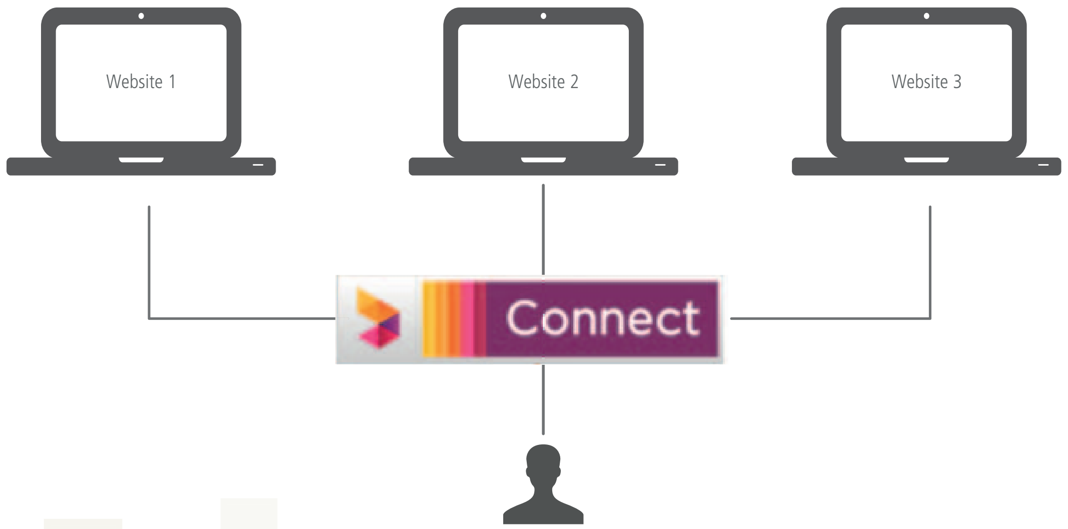
Dialog, part of the Axiata Group, is Sri Lanka's leading mobile operator by subscriber numbers, and also one of the leading operators in the region in terms of innovation. Since its launch in 1995, Dialog has moved from being the fourth licensed operator to being market leader, with a market share of 38% (equivalent to over 7.5 million subscribers). With a strong drive towards the innovative use of mobile technologies, carefully contextualised to the Sri Lankan market, the company has achieved considerable success. The company operates GSM, GPRS, EDGE, W-CDMA and 4G LTE communications networks, and was the first company to launch commercial 3G and HSPA+ operations in South Asia. When Dialog announced that it had switched on its 4G network in Colombo, it became the first LTE network in South Asia.

In addition to its core business of mobile telephony, Dialog operates a portfolio of services including Dialog TV, the country's leading direct-to-home satellite TV service, and Dialog Global which provides international telecommunication services. Dialog Broadband offers fixed-line broadband internet services, whilst Dialog Tele-Infrastructure is the company's national infrastructure arm. In March 2013, the company announced the launch of its own Dialog Branded Smartphone series at an entry price point of less than Rs. 10,000. The Dialog i-Series Android 2.3 Smartphones come preloaded with a range of Dialog Apps like MyTV, Dapp, Traveloid and represent a strategic push to drive mass adoption of Smartphones across the country.

Dialog was the first mobile operator to cover the Jaffna Peninsula in Northern Sri Lanka, within 90 days of the ceasefire agreement in 2002 and, in 2009, was the first mobile operator to extend its network to the areas in the North and East Province where the war was fought. It presently has 80% market share in these regions, and has contributed materially to their recovery from hostilities.

Identity sits at the heart of Dialog's strategy, and digital identity forms an increasingly substantial part of the company's operations. The company's newly created Dialog Connect service is designed to bind each individual subscriber to a unique, secure persona – which can be applied across multiple platforms and in relation to a wide and growing range of service providers.

Dialog's vision is to create a unified identity solution that individual users can trust as a means of securely verifying their identity across multiple networks, platforms and service providers.



II Telecommunications in Sri Lanka

A. High mobile penetration:

Though Sri Lanka is considered a developing nation, it has nonetheless emerged rapidly as a forward-looking economy in which the power of technology is leveraged to its fullest extent by both public and private sector institutions. With mobile subscription penetration nudging 50% and penetration rates increasing rapidly[1], with many mobile subscribers having two SIM cards, mobile has already established itself as the single most important medium for communications and connectivity in the country. Recognising the potential of mobile, the government is helping to drive adoption, and amongst other things, hopes to raise smartphone penetration to 80% of active mobile subscribers within 2 years.

B. Growing internet penetration:

The government's desire to increase smartphone penetration is informed, at least in part, by relatively low internet penetration. Less than 10% of the population of Sri Lanka makes regular use of the internet, although mobile broadband penetration has already exceeded fixed line broadband penetration[2]. Both the government and the country's mobile operators are keen to see this figure rise rapidly, so that individuals and enterprises can take greater advantage of the global, digital economy.

Though fixed-line penetration is higher than much of the developing world (at around 20%), fixed broadband services rarely extend beyond main urban centres, whereas mobile broadband coverage extends to much of the country's landmass. Nonetheless, online commerce, internet banking and access to e-government services remain the preserve of a small minority of the population.

For the most part, this is because internet access remains a relatively new phenomenon for the majority of the population. This is partly as a result of the country's recent history, and perhaps equally importantly, partly because very few websites are available in Sri Lanka's two most dominant languages, Singhalese and Tamil.

As a result, though there is considerable interest in and enthusiasm for the internet and the digital economy at large, there remain material practical barriers to adoption. As is the case in many other emerging economies, the mobile medium is expected to dominate the broadband and internet access markets. This is due to the comparatively low level of household PC penetration (around 10%), the comparatively lower cost of mobile smartphones, the ubiquitous nature of mobile coverage, and the growing increment between fixed broadband and mobile broadband connection speeds (4G mobile networks in Sri Lanka are already offering download speeds of approaching 50mbps, whereas fixed broadband suppliers offer considerably slower speeds, to a small fraction of the population). A full third of mobile subscribers already have a 3G mobile subscription.

Mobile operators, Dialog in particular, have therefore adopted an aggressively forward-looking stance in relation to broadband connectivity, internet access and associated issues. Since 2012, Dialog has offered its customers the capacity to pay for goods and services in the real world using their mobile phone. The company's eZCash service is today used by over 930,000 people, to pay for utility bills including Dialog bills as well as to send money home. Transitioning to the online world, and providing identity verification / authentication services in support of a wider, deeper range of services, products and content, was a logical, sequential step for the company.

World Bank Social Indicators, Sri Lanka, 2010

Population	21 Million
Landmass	65,610 square kilometres
Population Density	329 people per square kilometre
GDP	USD 59 billion
GDP per Capita	USD 2,864
Mobile Subscriptions	9 million
SIMs per Subscriber	2
Mobile Coverage	Circa 95%
Network Technologies	2G, 3G (W-CDMA), 4G (LTE)
Fixed Line Penetration	Circa 20%
Internet Penetration	Circa 12%
Number of ISPs	50+
PC Penetration	< 10% of households
Rural population (% of total)	85%

[1] Sri Lanka's mobile penetration rate increased by a factor of over 1.5x between 2008 and 2010. GSMA Asia Mobile Observatory 2011.

[2] GSMA Asia Mobile Observatory 2011.

III Identity in Sri Lanka

C. Identity cards

It is a legal requirement for all citizens of Sri Lanka over the age of 16 to possess a National Identity Card (NIC). ID cards are issued by the Registration of Persons Department, which sits under the Ministry of the Interior. Each NIC has a unique 9-digit number, in the format 000000000A (where 0 is a digit and A is a letter). The first two digits represent the citizen's year of birth (88xxxxxxxx for someone born in 1988).

By law, all citizens are required to carry their identity card on their person at all times, as proof of identity. Over time, the need to carry a physical identity card proved problematic: the stock of cards currently in use are laminated paper, and therefore comparatively simple in nature, easily tampered with, and readily lost or damaged.

D. National identity registry

The state also initiated a project to create and maintain a consolidated database comprising a 'Population Register', containing the unique ID numbers and basic information of all citizens. This formed part of wide-ranging government efforts to modernise social infrastructure, partly in response to the end of civil unrest, and partly in order to accommodate the challenging characteristics of the country (for example, over 85% of the population of Sri Lanka is rural, and it has historically been difficult for the government to serve citizens in remote areas). The government's population register database was designed to create a contemporary, accurate and dynamic database of the entire population, which was sufficiently flexible to capture and reflect changes (such as births, deaths, marriages, changes of address) in near real time.[3]

These and other activities have led to a steady transformation of the Sri Lankan state, as technology has been used to address the 'generic' challenges associated with emerging economies, and the specific challenges relating to Sri Lanka's geography, population structure, state infrastructure and so on.

A critically important side-effect of the government's programmes has been to place mobile operators – and Dialog in particular (as the largest operator in the country, with over 38% market share) – at the forefront of identity management, a position which has helped operators to earn considerable trust amongst consumers, government and the broader enterprise market.

E. Innovative identity solutions

In 2009, at the end of Sri Lanka's decade-long civil war, a government-mandated initiative required each citizen to carry a physical copy of their mobile connection registration to prove that they were the owner of the SIM card. This would require each mobile operator to call in subscribers to re-register their SIM cards in-store. With over 5 million subscribers at the time, Dialog knew that it would be impossible to physically re-register all of its subscribers within the short time frame. The company developed its #132# solution as a means of resolving this mandate: Dialog already held soft copies of the national identity documentation used by each customer to subscribe to their mobile service (birth certificate, passport, billing proof, etc.).

By dialling the #132# USSD short-code, any Dialog subscriber could pull their personal information –collected at the point of sale and stored in a secure server – onto their mobile device. With a 3rd step, customers could notify the company of incorrect information and come in person to update their personal information with supporting documents. Dialog issued its own electronic certificates for the #132# code, which are stored in a server and pushed to the user when they dialled the USSD code.

In this way, customers had a way to link the physical ID they carried already with the phone ID without needing to register for a second identification document.

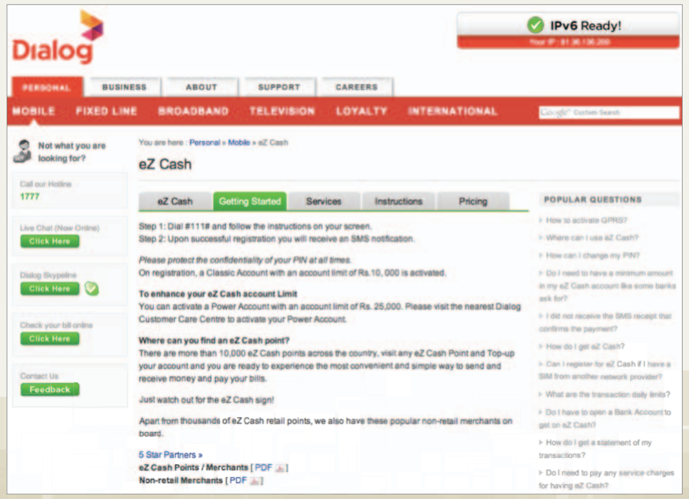
Within the first six months of 2009, Dialog recorded 18.5 million #132# dials as people used their mobile to prove who they were . Even though the government mandate is over, they still have 700 to 800,000 hits per year as customers check up on their data. This service was amongst the first in the world to bind government-issued identity credentials to a mobile-operator deployed service.

[3] ePopulation Register (http://www.icta.lk/en/programmes/re-engineering-government/131-main-projects/251-epopulation-registry-.html)

eZ Cash: Verified customer data for mobile money

Amongst Dialog's most innovative services is their eZCash, mobile money service (formerly eZ Pay). Mobile money has been a particularly important service as Sri Lanka transitions socially and economically. Bank account penetration is around 57%, but remains low in rural areas. As a result, mobile money services have become an important lifeline for citizens.

Dialog's eZCash service, in and of itself, has an important identity component. Following Dialog's launch of eZ Pay in partnership with the National Development Bank in 2007, the Central Bank began to develop a regulatory framework for mobile money that allowed both banks and MNOs to operate mobile money services. In April 2012, Dialog was awarded a license from the Central Bank and, two months later, launched eZ Cash as a fully telco-led mobile money service.



You are here : Personal » Mobile » eZ Cash

eZ Cash

Step 1: Dial #111# and follow the instructions on your screen.
Step 2: Upon successful registration you will receive an SMS notification.

Please protect the confidentiality of your PIN at all times.
On registration, a Classic Account with an account limit of Rs.10, 000 is activated.

To enhance your eZ Cash account Limit
You can activate a Power Account with an account limit of Rs. 25,000. Please visit the nearest Dialog Customer Care Centre to activate your Power Account.

Where can you find an eZ Cash point?
There are more than 10,000 eZ Cash points across the country, visit any eZ Cash Point and Top-up your account and you are ready to experience the most convenient and simple way to send and receive money and pay your bills.

Just watch out for the eZ Cash sign!

Apart from thousands of eZ Cash retail points, we also have these popular non-retail merchants on board.

5 Star Partners »
eZ Cash Points / Merchants [PDF]
Non-retail Merchants [PDF]

POPULAR QUESTIONS
- How to activate GPRS?
- Where can I use eZ Cash?
- How can I change my PIN?
- Do I need to have a minimum amount in my eZ Cash account like some banks ask for?
- I did not receive the SMS receipt that confirms the payment?
- How do I get eZ Cash?
- Can I register for eZ Cash if I have a SIM from another network provider?
- What are the transaction daily limits?
- Do I have to open a Bank Account to get on eZ Cash?
- How do I get a statement of my transactions?
- Do I need to pay any service charges for having eZ Cash?

In adopting a more proportionate approach to customer due diligence in the KYC (Know Your Customer) requirements, this regulatory change had significant positive implications for Dialog. Customers can sign up for a "Basic Account" on their mobile phone using the ID already stored in Dialog SIM card registration database. Basic Accounts are self-registered which means you do not need to attend a mobile money agent. The maximum transaction allowed with this account is 10,000 rupees (US$80), but customers can make more transactions by upgrading to a "Power Account"; they simply need to reconfirm their identity at a mobile money agent. By June 2012, more than 370,000 customers had signed up to eZ Cash (up from 15,000 only a few months earlier), reaching 810,000 by early 2013. 4,000 of these customers have already signed up for a "Power Account".

In essence, Dialog leveraged its strong, existing customer registration process – as well as its large retail and dealership presence – to outstanding effect. There are around 12,000 registered eZCash points across the country for money-in and money-out services. Whereas retail banks and credit card companies had not managed to extend their reach much beyond major urban centres, Dialog deployed its mobile money service across its entire footprint, which covers over 95% of the population, and has brought financial services to many citizens for the first time ever.

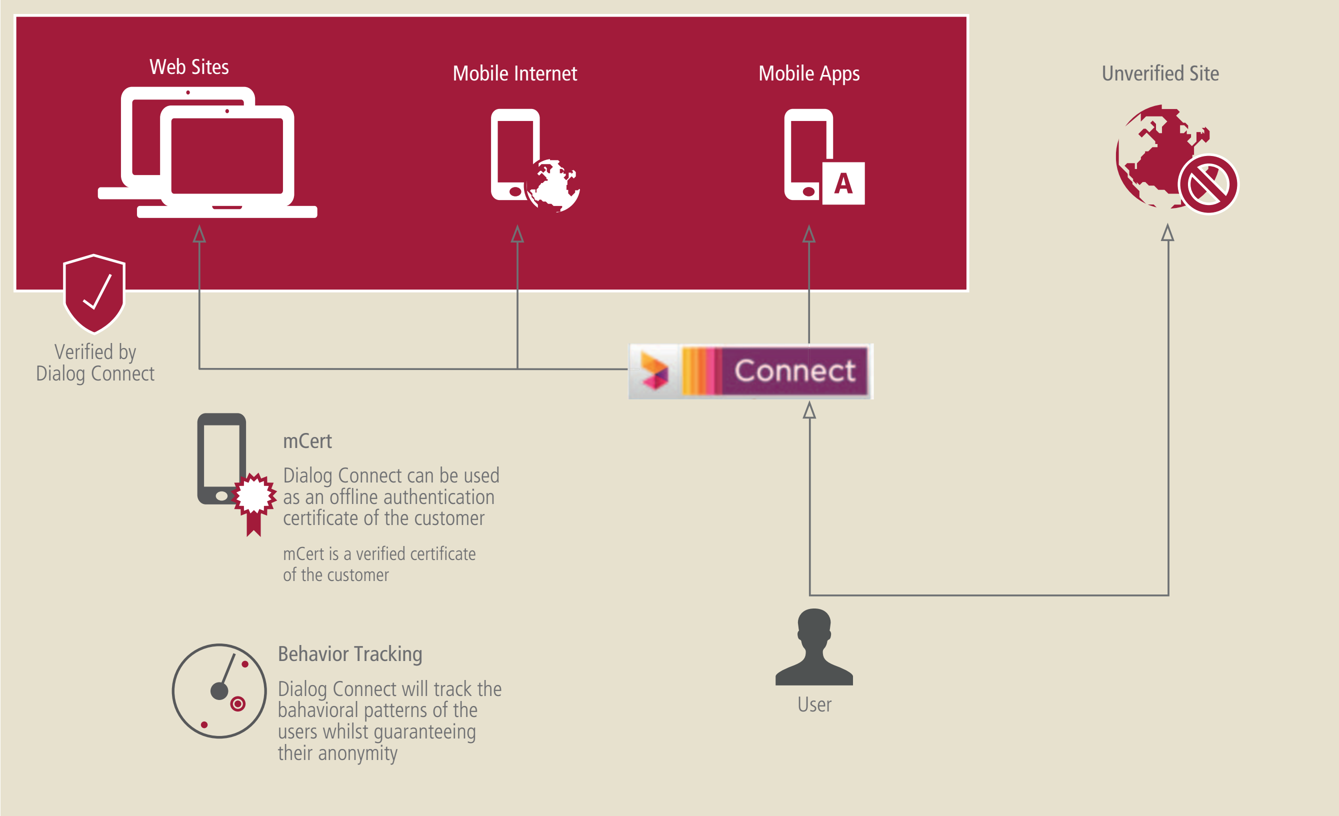
IV Dialog Connect: Dialog's Mobile Identity Service

As was the case with the #132# service, the eZCash service placed Dialog in a strong strategic position – and indeed in a position of considerable trust – within the realm of identity and its management. This caused the company's management to examine the notion of identity management – as an enabler and as a service in its own right – in greater depth. A process of research, planning and customer research led Dialog to a clear conclusion. Sri Lankan citizens needed a means to prove or authenticate their identity for a wide range of purposes, spanning existing services (such as eZCash) through to entirely new arenas (such as buying goods and services online). The result of this strategic vision was Dialog Connect, an identity authentication solution that works across a variety of platforms, use cases and service providers.

A. Vision, Principle and Benefits

i. Dialog Connect is an easy-to-use identity authentication solution through which use rs can verify their identity across multiple platforms, use cases and third party service providers. The service is designed to further leverage Dialog's strong registration process and deliver event-based authentication for third party service providers, along with profiling data with a high level of assurance.

Based on the OAuth standard, which is widely used by online service providers, the Connect service creates a federated digital identity for the subscriber, which can be used as an authentication token to log in to all participating third parties. In other words, the subscriber creates a single Dialog Connect ID, which can be used within the context of a wide range of service providers, and their respective products and services.



Dialog Connect can be used as an offline authentication certificate of the customer

mCert is a verified certificate of the customer

Dialog Connect will track the bahavioral patterns of the users whilst guaranteeing their anonymity

ii. The benefits to subscribers are manifold:

(1) The subscriber does not need to create a unique username and password for each service provider that he or she uses; there is therefore reduced "login fatigue".

(2) The subscriber's identity data is protected and managed by the Connect service; so for example, if a service provider requests personal information (name, age, gender) from the subscriber during the login process, the subscriber is specifically asked if he or she wishes to comply and continue using the service or whether he or whether he or she prefers to keep the information confidential and thus avoid using the service.

(3) The service minimises the registration effort by prepopulating many fields by using data shared by Dialog Connect.

(4) The service is symmetric – not only does it authenticate the subscriber, but it also verifies each service provider, at each usage attempt (so the user's exposure to phishing attacks and the like is minimised).

(5) Identity tokens used for each session last only one session – therefore any token stored (accidentally or deliberately) after a log in is useless for future sessions (meaning that even if the device is stolen, the token is useless).

iii. Similarly, for service providers, the benefits are considerable:

(1) The service provider gains access to Sri Lanka's single largest integrated customer base.

(2) The service provider is offered profiling data so that they can refine and customise their offerings to individual consumers or groups thereof.

(3) The service provider enjoys a high level of assurance in relation to subscribers' personal profile data/attributes.

(4) The service provider attains a higher level of security in preventing fraud due to the strong authentication via two factor authentication. In future, the smartphone identity component will be tightly coupled to the SIM.

(5) The service provider gains easy integration to additional Dialog services (e.g. SMS notifications, Click2Call etc) which can also be authenticated using Dialog Connect.

In short, the Dialog Connect service is designed to help bridge the digital divide. In Sri Lanka, as in much of the developing world, the digital divide is less about access to connectivity – mobile coverage is almost ubiquitous and mobile SIM/device penetration extends to the majority of the population. Instead, the digital divide derives from the relative lack of identity mechanisms, and specifically, lack of verified financial/banking identity, which is required to buy and sell online.

Additionally, lack of trust on the part of both consumers and service providers in existing banking and payment processes has created a natural space into which mobile operators – as ubiquitous and trusted brands with strong customer care processes and wide-spread local distribution networks – can play a significant role in the development of a convenient and dependable solution for online access. Dialog Connect creates both the identity platform and a corresponding secure authentication mechanism which allows Sri Lankan citizens to participate more fully in the digital economy, and the internet at large.

Dialog of course deployed the service on the basis of commercial, not charitable, objectives. Mr Anthony Rodrigo, Group Chief Information Officer at Dialog summed up the benefits of the service to the company as follows:

"Dialog Connect is a key component of our platform strategy. By tightly coupling our payment tools and other service offerings, we can drive usage of these direct revenue-generating services. In addition, utilising the Dialog identity across multiple third party sites will contribute significantly to churn reduction."

B. How it works – registration

For Dialog's own customers, access to the Connect service is granted after successful completion of a strong registration process (the same process employed when an individual wishes to subscribe to Dialog's mobile network). When subscribing to Dialog's network, each customer is required to present:

– National Identity Card or a valid passport

– Proof of address (if different to the address stored on the ID card)

At the point of registration to Dialog Connect, the user is required to provide their mobile number. A validation PIN (generated as a one-time password) is subsequently sent to the subscriber, which the subscriber is required to use in order to activate their account (via the Dialog Connect web portal, which can be accessed via a PC, in store). This step verifies that the user is in possession of the MSISDN associated with the Dialog Connect account at the point of registration. Subsequently, once this verification is complete, the Dialog Connect account and the user profile in the Dialog billing system are joined and synchronised: creating a single, secure identity.

C. How it works – technology

Dialog connect uses an OAuth-based architecture to securely expose user information to verified clients. OAuth is an open standard for authorisation online. In overview, the OAuth framework enables a third-party application to obtain limited access to a resource (i.e. user information), on behalf of an end-user (the Connect service subscriber, the resource owner) by executing an approval interaction between the user and the service provider.

In short, what this means is the OAuth provides a standardized framework for the exchange of user information between a resource owner (Connect subscriber) and service provider (Web sites, Mobile Apps, etc.) without sharing the user's credentials. This avoids the storage of user credentials on multiple services, which of course represents a security risk. The credentials and information will only be stored within Dialog Connect.

Instead, the OAuth standard never shares users' credentials across the internet or on corporations' servers: rather, it relies on a trusted third party (in this case Dialog) to issue an authentication token to the service provider, which allows the subscriber to gain access without creating or sharing a username or password with that service provider. As mentioned earlier, each authentication token expires immediately after use and is therefore of no value to a criminal (whereas a username and password are).

The OAuth schematic above describes the following steps:

1. The end user goes to the URL of the company. The company's servers request authorisation from the user. The authorisation request can be made directly to the user (as shown in the schematic), or indirectly via an authorisation server (which would be owned/operated by Dialog).
2. The company's server receives an authorisation grant, which is a credential representing the user's authorisation, and is connected to an authorisation server.
3. The company's server requests an access token by authenticating with the authorisation server and presenting the authorisation grant.
4. The authorisation server authenticates the client and validates the authorisation grant, and if valid, issues an access token.

Under the auspices of this approach, the user (the Dialog Connect subscriber) can gain authenticated access to a website, without (a) creating an identity on that site or (b) sharing personal information or attributes with the owner of the website. All that is passed to the owner of the site is an authentication token – in many instances, the website owner will never know any element of the identity of the individual to which the token refers.

The token becomes invalid and unusable as soon as it has been used in a single authentication process, thus none of the website owner's servers retains data that could compromise the identity of the end-user.

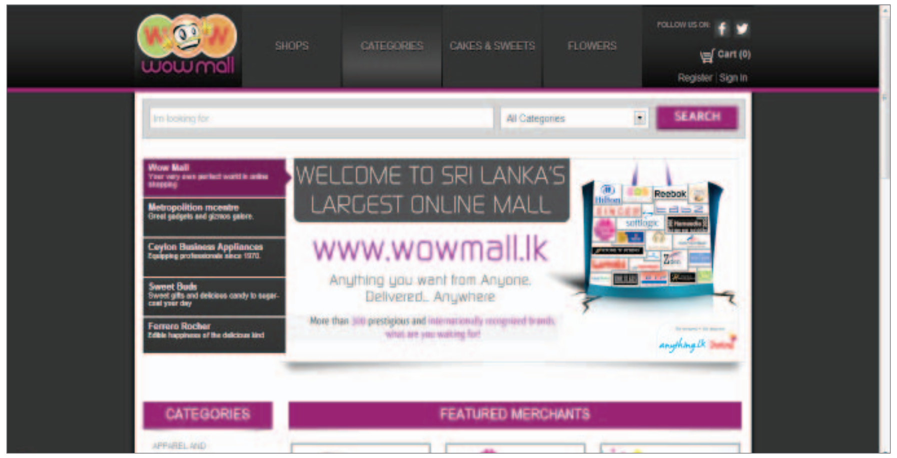
Dialog has added a number of features on top of the underlying OAuth code, so as to further secure both the identity of their Connect service users and the integrity of any transactions taking place over the system. So for example, the Connect service also offers the ability to provide a second authentication factor, for use cases that require infer a higher level of risk or in which a higher value transaction is being undertaken (both of which are typically characteristics of ecommerce). Under this second factor solution, a one-time password (a PIN code) is sent to the mobile number registered under the Dialog Connect account. The user is required to enter that PIN code in order to complete a transaction. This minimizes the risk of stolen user credentials, and fraudulent use of a stolen device.

Further, so as to avoid improper or unauthorised use of the service, the Dialog Connect account is configured to automatically issue an SMS to the MSISDN of the account holder every time a login attempt is made.

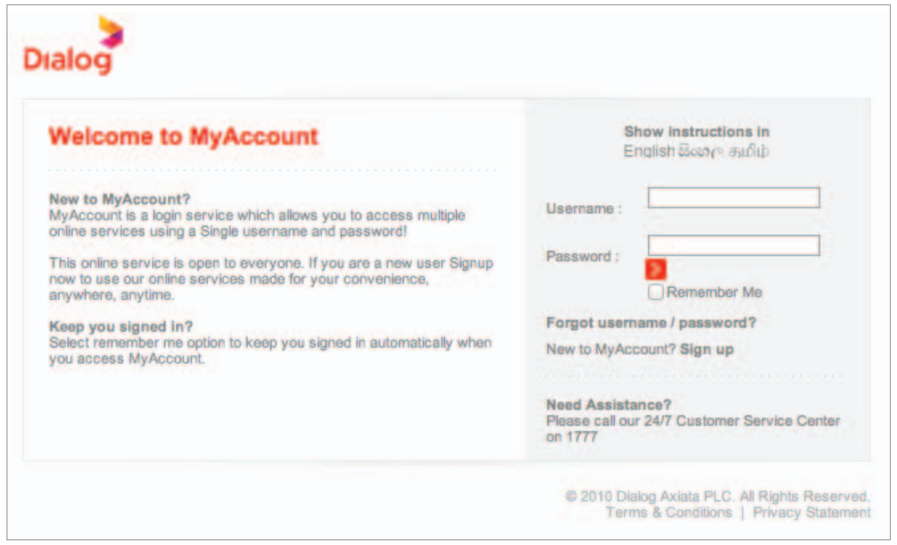
D. How it works – the user experience

From the perspective of the end user, the Dialog Connect experience is straightforward. The registration process is necessary in order to underpin the trust implied by the OAuth standard (if the third party website operator does not trust the token issued by the operator, or does not believe that the token pertains to a real human being, the system cannot work). Strong and strictly monitored registration is therefore critical.

Once registered, use of the service is straightforward. The user goes to a participating website (a website that has become a Dialog Connect partner), as illustrated right.


wow mall
SHOPS
CATEGORIES
CAKES & SWEETS
FLOWERS
FOLLOW US ON:
Cart (0)
Register | Sign In
Im looking for
All Categories
SEARCH
Wow Mall
Your very own perfect world in online shopping
Metropolition mcentre
Great gadgets and gizmos galore.
Ceylon Business Appliances
Equipping professionals since 1970.
Sweet Buds
Sweet gifts and delicious candy to sugar-coat your day
Ferrero Rocher
Edible happiness of the delicious kind
WELCOME TO SRI LANKA'S LARGEST ONLINE MALL
www.wowmall.lk
Anything you want from Anyone. Delivered.. Anywhere
More than 300 prestigious and internationally recognized brands, what are you waiting for!
anything.lk
CATEGORIES
FEATURED MERCHANTS
APPAREL AND

The user clicks the Dialog Connect button on the site, and is presented with the following –


Dialog

Welcome to MyAccount

New to MyAccount?
MyAccount is a login service which allows you to access multiple online services using a Single username and password!

This online service is open to everyone. If you are a new user Signup now to use our online services made for your convenience, anywhere, anytime.

Keep you signed in?
Select remember me option to keep you signed in automatically when you access MyAccount.

Show instructions in
English සිංහල தமிழ்

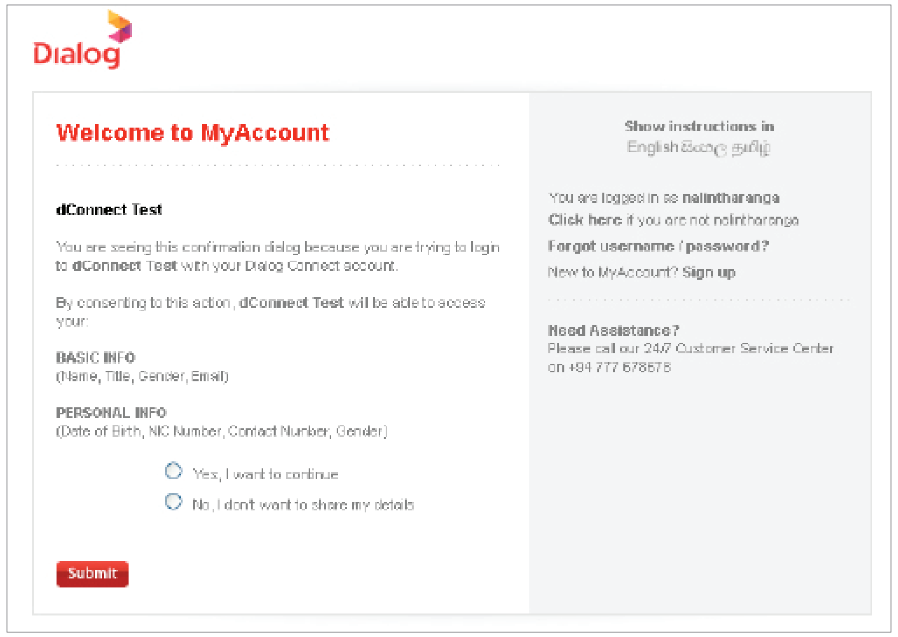
Username :
Password :
□ Remember Me

Forgot username / password?
New to MyAccount? **Sign up**

Need Assistance?
Please call our 24/7 Customer Service Center on 1777

© 2010 Dialog Axiata PLC. All Rights Reserved.
Terms & Conditions | Privacy Statement

The user enters their username and password, and is then guided to a consent page, shown opposite. The purpose of this page is to specifically request user consent for the sharing of personal information, requested by the third party service provider. The majority of end-users are quite happy to share basic, minimum information about themselves, particularly in return for discounts, deals and other benefits. But the Dialog Connect service, importantly, gives them the choice not to share if they have specific privacy concerns.


Dialog

Welcome to MyAccount

dConnect Test

You are seeing this confirmation dialog because you are trying to login to **dConnect Test** with your Dialog Connect account.

By consenting to this action , **dConnect Test** will be able to access your:

BASIC INFO
(Name, Title, Gender, Email)

PERSONAL INFO
(Date of Birth, NIC Number, Contact Number, Gender)

○ Yes, I want to continue
○ No , I dont want to share my details

Submit

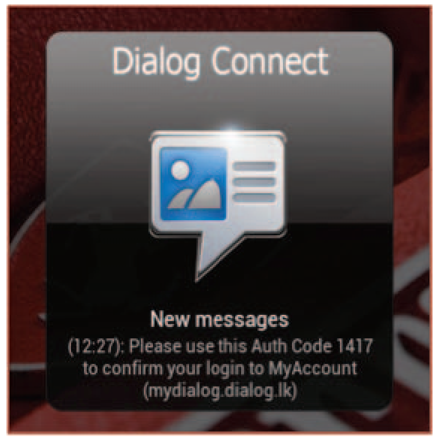
Show instructions in
English සිංහල தமிழ்

You are logged in as **nalintharanga**
Click here if you are not nalintharanga
Forgot username / password?
New to MyAccount? **Sign up**

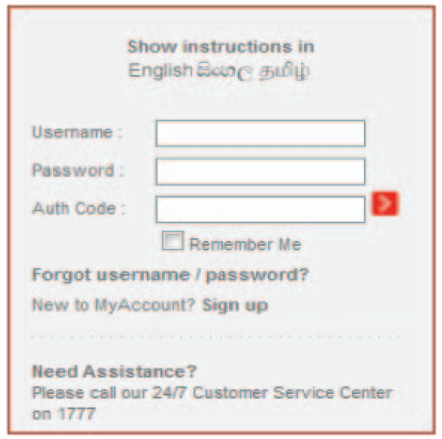
Need Assistance?
Please call our 24/7 Customer Service Center on +94 777 678678

As soon as the user clicks submit, their identity has been authenticated, a token passed, and they are registered on the website. Should they wish to make a purchase, they will be required to follow the second factor authentication process, which (as set out earlier), requires the user to enter a one-time password (PIN code) to authenticate a transaction.

In this instance, the PIN is sent to the phone – whereas the transaction is occurring on a separate device (typically a personal computer). The provision of a correct PIN code gives the service provider comfort that the end user is a legitimate and legal person, and that the transaction is genuine, and gives the end-user comfort that the transaction is being executed securely, with full non-repudiation should something go amiss (for example, if a purchased product is faulty, incomplete or not delivered).


Dialog Connect

New messages
(12:27): Please use this Auth Code 1417 to confirm your login to MyAccount (mydialog.dialog.lk)


Show instructions in
English සිංහල தமிழ்

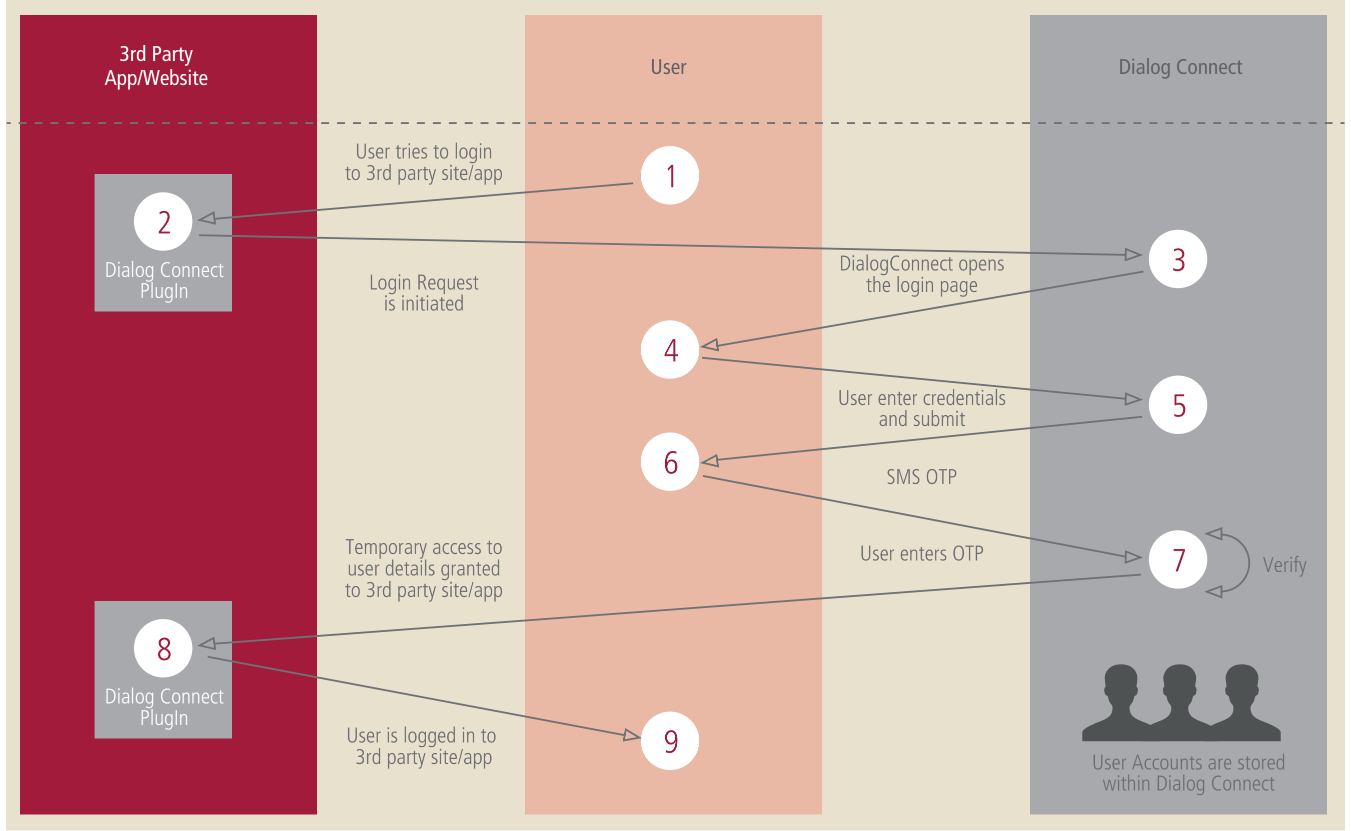
Username :
Password :
Auth Code :
□ Remember Me

Forgot username / password?
New to MyAccount? **Sign up**

Need Assistance?
Please call our 24/7 Customer Service Center on 1777

It is instructive to look at the end user experience from the perspective of information flows and exchanges, as this illustrates the logic of the underlying OAuth standard, and the lengths to which it goes to ensure that the integrity of an individual's identity is respected and protected online. These information flows are illustrated in the diagram below.

In summary, in its present form, the Dialog Connect service offers a convenient and secure means of allowing users to create and apply a digital identity, rooted in their mobile account, that can be used as a means of logging in to a growing range of third party websites.


3rd Party App/Website
User
Dialog Connect
User tries to login to 3rd party site/app
1
2
Dialog Connect PlugIn
3
DialogConnect opens the login page
Login Request is initiated
4
User enter credentials and submit
5
6
SMS OTP
Temporary access to user details granted to 3rd party site/app
User enters OTP
7
Verify
8
Dialog Connect PlugIn
9
User is logged in to 3rd party site/app
User Accounts are stored within Dialog Connect

Going Forward: Future mobile identity services

OpenID

Going forward Dialog Connect will be enhanced to include the OpenID web standard. Adopting OpenID will allow the service to function with a wider range of participating websites, who already use OpenID. Interestingly, the OpenID standard is also used by a variety of social media websites, and incorporation of OpenID within Dialog Connect will provide easy integration and enable interworking with a larger number of sites.

Social Network login

In addition to login and registration directly via Connect, Social network login such as Facebook Connect could be used to authenticate the user when registering to Dialog Connect for the first time. This will enable Dialog to link the user's social network profile to their existing subscriber profile and also enable Social network integration (enabling posting of comments and likes etc) of the participating site.

Authentication for other Dialog Platforms

Once Dialog Connect authenticates a user, the company plans to use the underlying token to automatically authenticate the user into other Dialog services such as Add2Bill, Click2Call, SMS alerts and LBS. This will allow service providers to use multiple Dialog services with simpler integration and provide a richer user experience. In essence, it should have the effect of making Dialog Connect a one-stop shop for companies in Sri Lanka and elsewhere wanting to sell goods and services to Dialog customers online.

V Uptake and Scale

Since its launch in 2012, Dialog Connect has already managed to amass a base of over 400,000 subscribers. The achievement is all the more remarkable given the relative shortage of native Sri Lankan ecommerce service providers (which is problematic because of the specificity of Sri Lanka's two main indigenous languages, Tamil and Singhalese). However, Dialog is working with a number of local companies, and is targeting the launch of a native language music site, and an ebook store.

Dialog therefore faces challenges that are common to most of the existing providers of this type of service. There is almost always a "chicken and egg" problem: users are loath to sign up for a federated identity service that is not supported by a wide range of service providers, and service providers tend to adopt a "wait and see" approach until there is a large installed base of active users. The circumstances are slightly different in Sri Lanka, as Dialog is of sufficient size and importance that it has been able to (a) create its own ecommerce platform as a means of enticing users to adopt the service and (b) work with local companies to transition their propositions online.

A base of 400,000 Connect subscribers is still enticing to service providers, and by integrating with the Dialog Connect service, access to those customers is available from day one of live operation. Perhaps equally importantly, the inherent security of the Connect platform is attractive to service providers, particularly because of the integration of eZCash. For many service providers, the ability to transact securely via the end users mobile wallet is an extremely appealing proposition, particularly given the low level of bank account and credit/debit card penetration.

There is also considerable service provider interest in the (anonymous) customer profiling capabilities of the service, at the back end. Connect is able to tell service providers about the attributes or characteristics of the subscribers that visit their sites, and service providers, in turn are able to adapt everything from the products and services that they prioritise online through to the way those propositions are presented (visually) and the messaging around them.

From the perspective of consumers/end-users, the service has gained early popularity, but the company recognises that further investment in awareness and usage are required. Of the 400,000 subscribers already using the service, around 3,000 use the Connect service each day. On average, each of those users accesses 10 different services. Clearly, the company wishes to grow the total number of registered users, and the frequency of use of the service.

Part of the process of doing so is being addressed by recent efforts to better localise the service. As mentioned earlier, there are comparatively few (international) service providers that have adapted their offering to local Sri Lankan languages, and indeed, there are similarly few devices that are capable of presenting a Tamil or Singhalese user interface. Dialog is working with service providers, app developers and device manufacturers to overcome this important issue; and is focusing on a hybrid approach in which both languages are presented in roman characters (the alphabets of which are extensive and relatively complex).

VI Challenges

Awareness is arguably the greatest challenge that Dialog faces in commercialising its Connect service. Consumers are still at a relatively early stage on the learning curve relating to the digital economy, and do not yet recognise the potential that mobile identity can offer, within the context of ecommerce. Indeed, ecommerce in itself is still comparatively underdeveloped, and only a minority of the population is fully aware of its importance and potential.

Service providers are similarly not fully aware of ecommerce opportunities, nor the role of mobile identity (and its importance) within that context.

Those service providers that are more aware of ecommerce opportunities tend to default to the large, global names in the online world, such as Facebook, Google and others. In such companies they see quick access to a global audience; often forgetting that the registration process behind each identity carried by these and other companies is cursory, and unable to provide the same level of assurance and relevance as Dialog's Connect service. Circumstantially, Dialog has found it comparatively hard to persuade service providers that already use Facebook Login, for example, as to the value of Dialog Connect. In contrast, service providers that do not make use of global federated identity platforms are more understanding of the value of Dialog Connect's service.

It will likely take time for service providers to fully understand the extent to which Dialog Connect is differentiated from Facebook Login and similar offerings. Whereas Facebook does indeed have a massive customer base spanning almost all countries on the planet, its registration process is self-administered, and there is a comparatively low level of assurance that any given identity is real, or relates to a real human being. Whereas Dialog cannot match Facebook in terms of scale, it can certainly offer far higher assurance on the identity of the individual, because of the strength of its registration process. Ultimately, service providers will have to recognise that both solutions have relative merits (one scale, one assurance and relevance), and both (along with many others) will have to coexist.

Dialog IdeaMart

Application development, particularly in local indigenous languages, is gaining substantial ground in Sri Lanka. Dialog's developer community (called IdeaMart) alone has deployed over 1,000 applications, most of them designed to work on feature phones, which predominate in Sri Lanka at present. As the installed base of devices changes, it is expected that a growing range of smartphone apps will be developed and deployed.

IdeaMart developers currently use Dialog Connect to subscribe to the company's application programming interfaces (APIs). Going forward, to promote wider use and integration of Connect, API access also will be bound to Dialog Connect, with apps using OAuth compliant access tokens provided by Dialog (so use of the applications will require the subscriber to have a Dialog Connect account).

An Android application authentication module for Connect is also being developed, which will be tightly coupled to the SIM, adding a higher degree of security and also simplifying the login process.

VII Economics

The business model for the Connect service has multiple layers. Whereas consumers pay nothing to subscribe to the service, revenue is generated from the incremental increase in use of complimentary services offered by Dialog.

Customer profiling and market insight data generation is a further benefit of connect. This data can be shared with service providers in anonymous fashion to provide detail customer insight around their entire user base or around individual customers through sharing both demographic and usage data on clusters they belong too. This provides the capability for Service providers to launch targeted campaigns.

Furthermore, Dialog Connect generates value through intangible brand enhancement via the placement of the Dialog brand across multiple third party websites. As Dialog Connect becomes more widely adopted and becomes a more habitual part of a user's online behaviour, the company will contribute to churn reduction.

VIII Key Success Factors

A. Growing internet penetration and a need for trusted identity management

As elsewhere around the world, mobile and internet usage will only continue to grow rapidly in Sri Lanka. With government and other private sector entities committed to increasing broadband and smartphone access across the country, mobile operators are well-placed to bridge the link for their customers between mobile and online services.

While exposure to identity-based fraud and theft are only beginning to bring to light the inherent weaknesses in traditional methods for online login and access, users across the socio-economic spectrum in Sri Lanka have need for a service that enables easy, secure and convenient access to a broad array of online content. The combination of these factors created an ideal scenario for Dialog's launch of the Connect service.

B. Trust in mobile operators for identity management

Having set a precedent for obtaining and managing customer information in a secure and user-friendly fashion with the #132# solution and eZCash, Dialog has built a reputation for reliable and trustworthy service when it comes to identity management. Taking this to the next level with a simple, federated online access service was, on the one hand, a logical extension from the traditional realm of the mobile operator. At the same time, the service represents a strategically progressive approach by a mobile operator in firmly asserting their role in the m-commerce space, an arena from which operators have historically been excluded.

In this way, the Connect service represents an important step in defining new positions for mobile operators in the online and e-commerce market as the trusted third-party for secure, convenient identity management that sits directly in the hands of the consumer.

C. Dedication to innovation

Dialog's commitment to innovation – and willingness to dedicate significant time, effort and resources to building a service which falls traditionally outside the realm of the mobile operator – was a key factor in the early success of the Dialog Connect service. The service represents a culmination of many years dedicated to new service that push the boundaries of mobile services, while recognising and keeping the ever-changing needs of the customer closely in mind.

Mobile
Identity

For further information, please visit www.gsma.com/mobileidentity
or contact the GSMA Mobile Identity team at
mobileidentity@gsma.com