

Dialog Connect: Federating Identity for Today's Consumer

An Executive Summary



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. In Sri Lanka, a country with rapidly growing internet and smartphone penetration, Dialog launched Dialog Connect, a service enabling customers to use a single Dialog portal to sign in and authenticate themselves online for access to content and services via a wide range of third party partners. Since its launch in 2012, Dialog Connect has amassed a base of over 400,000 subscribers, around 3,000 of which use the service each day.

A number of factors have led to the early success of the service to date:

- The appeal of Dialog Connect for consumers lies in the ease of management of their digital identities. Dialog Connect is a form of “federated identity,” whereby the identity profile (or set of credentials) established with the operator at registration for their regular mobile subscription³ can be used to log in to all federated third parties (service providers such as Wowmall.lk, Sri Lanka’s largest online shopping site) using the OAuth open standard framework. Rather than needing to create a unique username and password for each service provider, the subscriber’s identity data is protected and managed by the Connect service through the issuance of an authentication token to the service provider, thus enabling the user to gain access to the site in one easy step and greatly increasing conversion rates – a particular point of value for service providers who worry about lengthy registration processes turning customers away.
- Dialog recognised early on that security of the service would be an important differentiator for service providers facing a growing online consumer base. 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. Security is further enhanced for financial transactions and other higher risk use cases through the use of a one-time-password (a PIN code) sent via SMS to the mobile number registered under the Dialog Connect account, which the user must enter into the online portal to complete a transaction – thus adding

a second factor of authentication to the process and minimising exposure to phishing attacks.

- Dialog understood the 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 they prioritise online through to the way those propositions are presented (visually) and the messaging around them. Service providers also gain easy integration to additional Dialog services (e.g. SMS notifications, Click2Call), which can also be authenticated using Dialog Connect. Service providers are charged a subscription fee as well as a percentage of the value of each transaction facilitated by the service.
- Part of Dialog’s success is due to the position of trust the operator has established among Sri Lankan citizens. In 2007, Dialog launched eZPay (now eZCash) in partnership with the National Development Bank, which enables customers to pay for goods and services (e.g. utility bills) using their mobile phone, as well as send money home. Dialog Connect is able to leverage this success and generate value through brand enhancement via the placement of the Dialog brand across multiple third party websites, which in turn is seen as a route to potential churn reduction.
- Dialog has a track record of providing easy solutions to daily inconveniences experienced by its customers. In 2009, Dialog overcame the challenge brought on by a government mandate on SIM registration, which required each citizen to carry a physical copy of their mobile connection registration to prove ownership of the SIM card. Dialog developed an easy solution for customers to check and demonstrate their correct SIM registration credentials via their mobile phone. By dialling a #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, as well as notify the operator of any incorrect information. Within the first six months of 2009, Dialog recorded 18.5 million #132# dials as people used their mobile to prove who they were.

Despite rapid uptake in the early months of the service, Dialog faces the same challenges confronted by many innovators in a new market. Service providers and consumers in Sri Lanka’s still relatively small e-commerce market do not yet fully understand the important role that secure identity management plays in today’s digital economy. Users are often reluctant 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. Those service providers that are more aware of e-commerce opportunities tend to default to the large, global names in the online world (e.g. Facebook and Google) for quick access to customers already using these services, often forgetting 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 Connect.

Dialog is working to overcome these challenges by promoting the service through its developer community, IdeaMart, encouraging developers to use Dialog Connect to subscribe to the company’s Application Programming Interfaces (APIs). Going forward, 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).

Dialog also plans to enhance Dialog Connect to include the OpenID web standard to allow the service to function with a wider range of participating websites, as well as potentially link social logins with the Dialog Connect login so that when a user logs in they can either use the social media login interface with additional authentication with Dialog Connect (providing extra security for the third party site, but a more familiar interface for the user) or use the Dialog Connect login to be able to post likes and comments on social media sites. Dialog is also looking at providing add-to-bill functionality, which is important for markets where credit card penetration is low, as well as exploring the potential of making the Dialog Connect service available to subscribers of other mobile networks to help drive uptake and scale.

Read about the case study in full and find out more about the Mobile Identity Programme on our website: www.gsma.com/mobileidentity/

¹ Today, over \$1 trillion of business is transacted online globally, but most e-commerce buyers and sellers have never met.
² Sri Lanka’s mobile penetration rate increased by a factor of over 1.5x between 2008 and 2010. GSMA Asia Mobile Observatory 2011.
³ When subscribing to Dialog’s network each customer is required to present their National ID Card or valid passport plus proof of address