Identity Now

Building a Digital Identity Ecosystem on Blockchain with SecureKey in the Telecommunications Industry
Few organizations have played as vital a role in reshaping our daily lives in the digital age as telecommunications companies. Smartphones and high speed wireless networks have fundamentally changed the foundation of both work and play, fibre optic networks provide speeds that were previously unimaginable, and 4K HDR content is more beautiful than ever.

At the same time, there are clear challenges for the industry ahead – pricing and revenue growth for wireline and wireless services are under pressure, with no easy cost reductions to offset this. While growing, “next wave” IoT services continue to be nascent. Add to this a changing regulatory environment that increases costs and lowers consumer trust. In this turbulent environment, telcos are increasingly looking to control costs, deliver on increased user expectations, and bring value add services above data connections.

Telcos are not alone in facing challenges as their industry matures. Financial services sector looked towards ABMs and online banking to reduce costs for basic transactions and increase the value of branch-based activities; airlines created loyalty programs to provide incremental value to customers which turned into new revenue streams. Now, recent technological innovations in digital identity provide an opportunity for telcos to increase digital adoption, reduce acquisition and support costs, and generate new revenue streams through ID validation services that users can control and value.

**Evolving Identity for the Digital World**

While telcos have been pushing the limits of technology for years, their ways of interacting with customers—primarily in-store and through call centres—have largely remained unchanged since the days before the iPhone. Online activations for many telcos remain in single digit percentages, and support often lands on call centres. The shift towards digital and self-serve channels has been hindered by a lack of reliable, low risk and convenient methods to validate a user’s identity.

It’s time to change—new digital identity ecosystems are coming, and telcos should be among the leaders and early adopters.

In late 2016, Canada’s six leading banks (RBC, CIBC, BMO, TD Bank, Scotiabank and Desjardins) joined an already impressive list of investors, including Rogers and Telus—two telecommunications companies in Canada, by providing $27 million in funding to SecureKey to develop a true digital identity and attribute sharing ecosystem. The new service enables secure and private attribute sharing through range a network of trusted parties including banks, credit bureaus, telcos, government, and more.

**The User Experience**

What could this mean when setting up wireless services with a new provider? Today, this process typically involves visiting a physical retail location with ID in hand, selecting the desired device and plan, then copying physical IDs and filling out forms, and setting up passphrases for the future. Porting the number can’t occur until the customer can provide their existing account number, often requiring a call to the call centre once home. The entire process can take in excess of 45 minutes – if things go smoothly.
Leveraging this identity ecosystem, new customers can visit the telco’s website, select the device they desire, consent to share their name, address and date of birth from their one bank, share their most recent credit score from a credit bureau, and their verified existing phone number. Delivery of the device is arranged for the next day, the line is immediately activated and porting can start as soon as the new device is turned on.

All of this can be done in a matter of minutes, directly from their smartphone, no matter where they are. No trip to a store, pictures of a driver’s license or lengthy forms to fill out. Users will control and authorize all sharing of information right from an app on their smartphone.

When customers need support, the same app can help reconfirm users regardless of channel—authorizing users without physical IDs or passphrases to remember. Digital channels can provide enhanced self-serve options while eliminating usernames and passwords, and messaging / chat bot platforms can be enabled without transmitting sensitive data through them.

Less time and effort is needed to validate customers, reps don’t need as extensive training, and customer experience is improved. Millions of dollars in benefits accrue from increasing online adoption, reducing friction for upsell / cross-sell, and lowering support costs. Customer experience scores improve as consumers are enabled across channels they want, and lower revenue IoT devices can be profitable through a lower cost to serve.

**Identity as a Service**

Digital identities also create opportunities for telcos to contribute assets to the ecosystem. Telcos are uniquely able to validate devices and SIMs on their network, their physical location, and that the device is not lost or stolen. Leveraging these, mobile network operators can provide a strong factor of authentication when needed, as has been recognized by the GSMA and carriers globally in services like Mobile Connect.

Where telcos have vetted customers (often postpaid accounts or wireline services) they too can provide profile attributes on a customer’s behalf in place of (or in addition to) banks and other institutions. For example, telcos know when customers move and new services are installed and can be a trusted source for this new address to other companies, with customers authorizing the transmission of such updates with few taps.

In both cases, telcos can provide information to help validate a customer in a transparent way with users in control, while earning a fee doing so. Monetization of data is an opportunity, but removing friction for customers and risk for businesses creates customer loyalty that’s of even greater value.
A short video highlighting the service can be found here:
https://youtu.be/9CxU1tghw0

Telcos can help drive this digital identity revolution. They are often trusted brands and have frequent touchpoints with customers—millions of customers sign up with providers every year, renew their services and/or have typical customer service interactions. Telcos can increase security and privacy for their users while reaping material cost savings.

The Business Model
The business model of the service is quite straightforward. The requestor of attributes pays for each set requested, and generally will request more than one validator to increase their business assurance. The providers of attributes get paid for each transaction they participate in.

For example, in order to provide the highest security to access healthcare records online, a hospital might request (a) name, address and mobile number from a tier one bank, (b) the name and health card number from the state or province, and (c) validation that the SIM in use is associated with the phone number of record at the bank, and that the device was not changed recently.

The network manages the billing and provides the vast majority of revenue back to the underlying providers of claims. The user provides explicit consent each time data is requested by a network participant (e.g., are you willing to share these attributes with this party for this purpose?). Each action is recorded in the ledger, and the user receives a secure notification on all actions.

Some sample attributes that we are enabling are shown in the diagram on the below.
The Technology

To achieve the goals of privacy, integrity and resiliency the service is being implemented on a private permissioned blockchain, with trusted partners running the peer nodes (e.g., each partner bank in Canada will run a node). Having run other identity ecosystems in Canada for many years, and having worked closely with both the U.S. Government on Connect. Gov and with the National Institute of Standards and Technology (NIST) on their new 800-63-3 guidelines, SecureKey felt this was the only way to solve the problem at scale.

Specific goals in the implementation include:

- That no data is visible to the operator of the network
- That there is no central database or “honeypot” of data
- That there is no central point of failure
- That there is privacy so that an Identity Provider cannot tell where an identity claim is being used.
- That there is no way to track an individual across relying parties.

SecureKey recently won grants for its architecture and approach from both U.S. Department of Homeland Security Science & Technology Directorate and the Canadian Government.

The foundation of the technology is built on Hyperledger Fabric, which is a blockchain framework and one of the Hyperledger projects hosted by The Linux Foundation. SecureKey has been working closely with IBM on the development of the technology, ensuring that it will be able to scale to meet global demands while respecting the core security, privacy, integrity, and resiliency aspects needed for an identity network. SecureKey’s implementation using IBM Blockchain is so that network participants will require very little blockchain operations experience, and it also allows the participants to quickly get on the high security business network with minimal effort.

The system’s decentralized nature eliminates single points of failure, dramatically improving resilience. Trusted parties from multiple industries can operate the nodes, while the system’s strong anonymity standards enable potential competitors to work together in the same ecosystem. Through these trusted parties, the network ensures privacy for individual users while maintaining convenience and ease of access.
**Entering Other Geographies**

The model is designed to be replicated in other geographies, and to meet their privacy and security regulations currently in place to protect their citizens. In Canada, SecureKey is already working on a number of valuable services for consumers, including:

- Telco Account Open
- Accessing Government Services
- Accessing Medical Records and Test Results
- Bank Account Open, Loan Origination and Transfer of Funds
- A Social Buying Network
- Apartment Rentals

Along with the above, more requests for new functionality are being received each day. The applicability to extend this functionality to organizations on a global scale is not only viable, but highly probable (and in fact already happening).

While there will be lots of incremental advantages for telcos in having a cross-border identity mechanism, the initial focus and benefit will be local.

**FAQs**

**Why hurry?**

The need for reliable digital identity solutions is increasingly pressing, and is critical to enabling the next wave of digital transformation for society as a whole. Many governments are looking towards public/private sector partnerships, and participants across industries are already stepping up. Telcos are coming from a strong position having been a reliable enabler for consumers and businesses alike in the digital age thus far. As the risk of being disintermediated by smartphone manufacturers or main OS providers increases, digital identity solutions represent a strong connection back to customers to continue delivering them value. To allow another party to enable strong identity use cases using smartphones before telcos do would be a lost opportunity.

**What is the business case for the telco?**

Telcos are set to benefit from being one of the biggest consumers of digital identity, and enabling a significant channel shift towards lower cost and automated online acquisition and support channels, without fraud. These benefits help lower existing costs while supporting new lower-ARPU growth areas such as IoT.

Additional opportunities exist for telcos to act as a source of identity and authentication, bringing new revenue streams, creating product stickiness and reducing churn. Finally, as solution providers, telcos can help proliferate these services to enterprise and government customers.
Why was a blockchain architecture chosen?
Privacy is vitally important. The system was built from the ground up on Privacy by Design principals. The attribute sharing party must, in most cases, not know where an individual is sharing their data. A distributed architecture provides resilience against denial of service attacks that will be vital in a nationwide identity ecosystem.

There had to be no way a central broker could be honest but curious (per NIST new guidelines). Having built both SecureKey Concierge in Canada and Connect.Gov in the U.S., there was no way to solve these characteristics well without blockchain. Having built both SecureKey Concierge™ in Canada and Connect.Gov in the U.S., it was determined that we couldn’t solve these characteristics well without blockchain.

Why not lead as a single telco?
For relying parties to come on board the solution requires ubiquity, and that means greater scale than any one telco can provide.

About SecureKey
SecureKey is a leading identity and authentication provider that simplifies consumer access to online services and applications. SecureKey’s next generation privacy-enhancing identity and authentication network enables consumers to conveniently assert identity information from trusted providers, like banks, telcos and governments, and help them connect to critical online services using a digital credential they already have and trust.