SECURE KEY

# Identity Data Exchanges Leveraging Blockchain Technology

Dmitry Barinov, CTO

# About SecureKey

- Founded in 2008
- Headquartered in Toronto, Ontario; offices in Ottawa, Montreal, Boston, San Francisco
- **Mission:** to build highly scalable trusted identity networks that enable organizations to quickly and easily deliver high-value online secure services
- Powering Major National Digital ID Networks in Canada, US and UK
- World-class group of venture and corporate investors, strategic partners

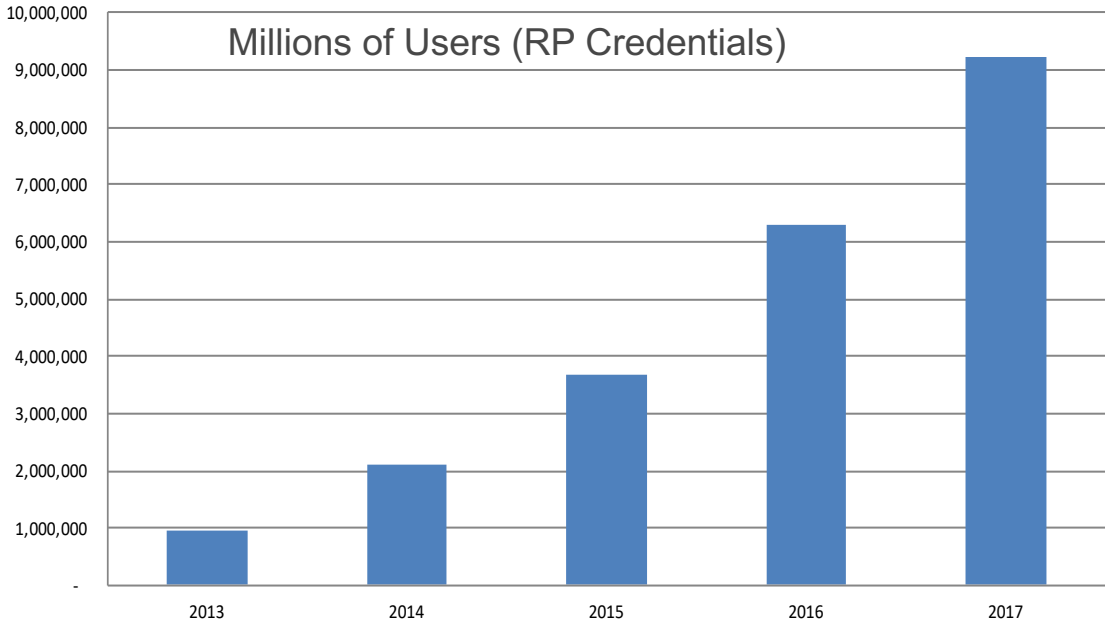
# Canada Started with Federated Login

SECURE KEY

## Millions of Canadians access government services using their known, trusted bank login

SECURE KEY Concierge

Leveraging Trusted & Familiar Bank Credentials To Access Other High-Value Services

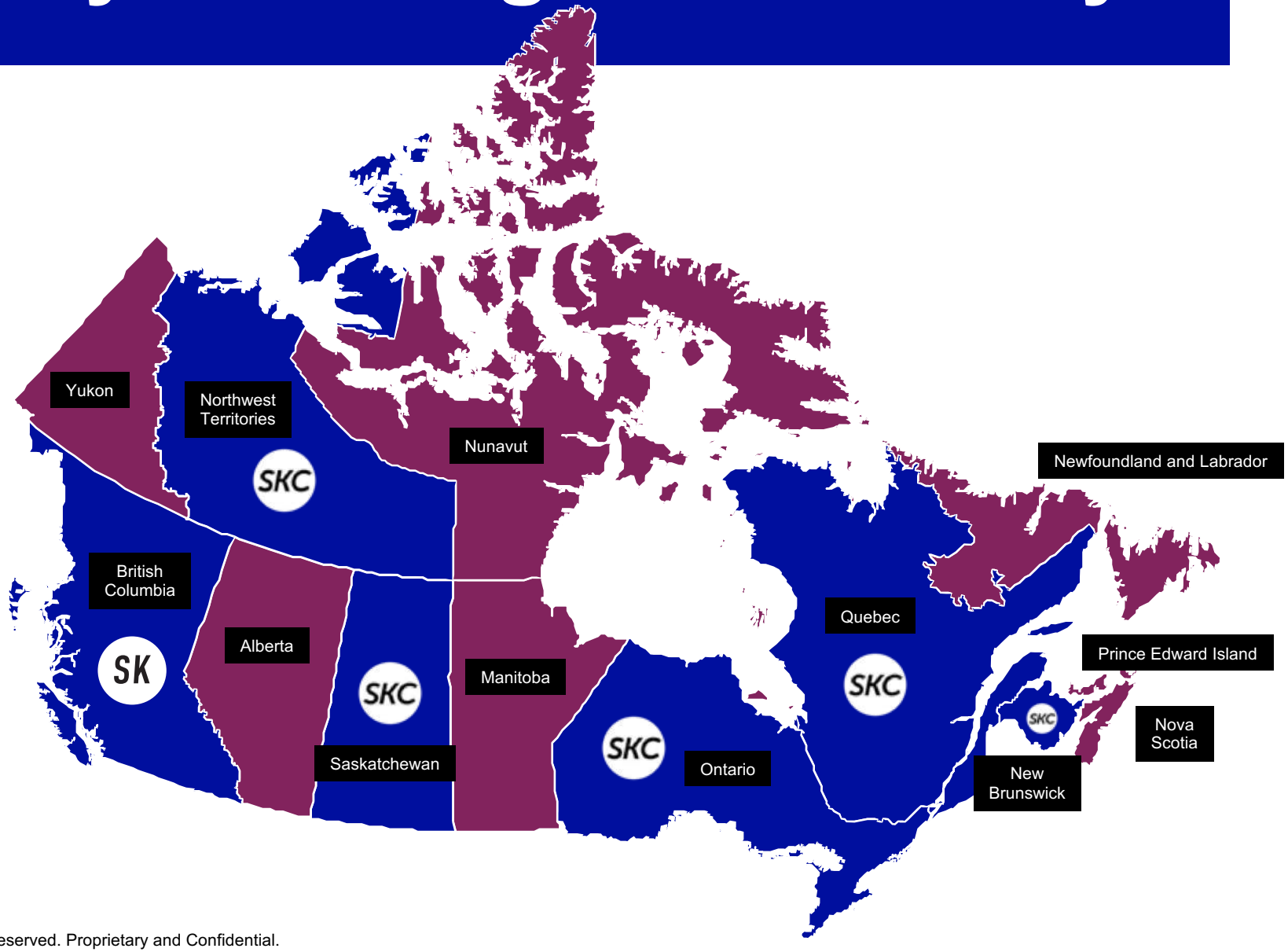




- Adding 200-400K credentials per month
- >80 Fed Govt applications, including CRA, Services Canada
- Revenu Quebec
- Provincials & Private Sectors
- Privacy by design (Triple Blind™)

PbD

# SecureKey Concierge Provincially

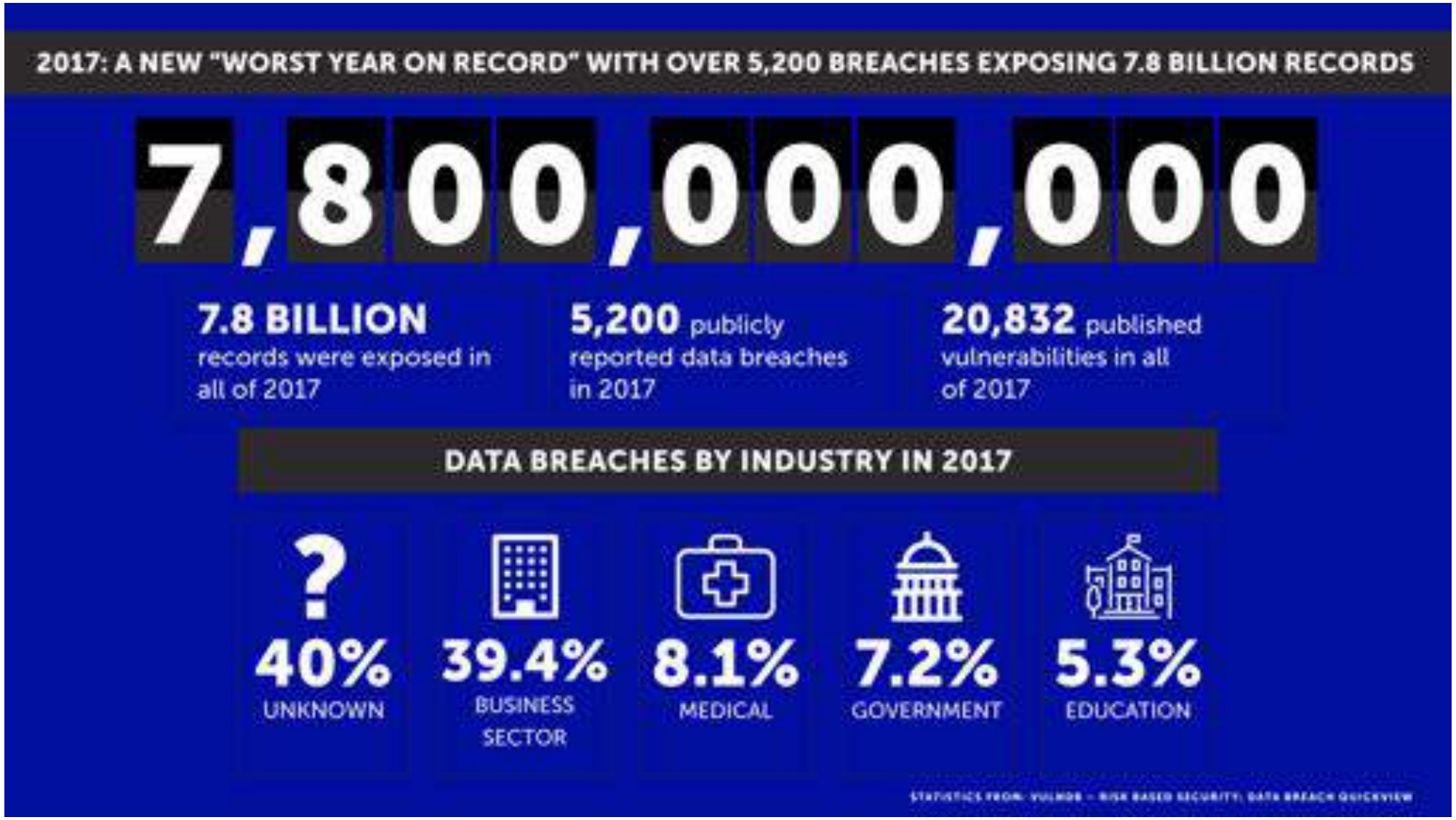



# Identity validation is broken

It needs to work in:

- Call centre
- In person
- Online

# Data Breaches 2017






Statistics from: VulnDB – Risk Based Security; Data Breach QuickView

# Driver's License: the Gold Standard?

vocativ

NEWS SCIENCE TECH CULTURE LIFE

CYBER SECURITY

# Hackers Spoof Samsung Iris Scanners With A Photo And Contact Lens

The new iris scanner on Samsung's Galaxy S8 makes it painfully easy for criminals to unlock your phone

By Joshua Kopstein

May 23, 2017 at 3:26 PM ET

The Telegraph

HOME NEWS

Technology

News Reviews Opinion Internet security Social media Apple Google

Technology

# Peace sign selfies could let hackers copy your fingerprints

Savvy fraudsters could recreate fingerprints from photos

By Cara McGoogan and Danielle Demetriou, TOKYO

12 JANUARY 2017 • 11:06AM

Researchers at Japan's National Institute of Informatics (NII) have found that fingerprints can be easily recreated from photos taken up to three metres away without the need for advanced technology. So long as the picture is clear and well-lit, prints can be mimicked.

Forbes / Security / #CyberSecurity


NOV 27, 2017 @ 05:10 AM 4,332 EDITOR'S PICK

# Apple Face ID 'Fooled Again' -- This Time

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

FULL BIO

*Researchers say Apple Face ID on the iPhone X isn't secure, but others wonder* [+]

The Vietnamese hackers who claimed earlier this month to have fooled Apple's Face ID with a mask costing less than $150 are back. But this time, their evidence is more compelling.

Whereas in their previous attack researchers from Vietnamese cybersecurity company Bkav didn't show the enrolment process, or how long it took from that point to opening an iPhone X with the mask, in a new proof of concept, they appear to do both. A video shows the Face ID facial recognition enrolment being reset. Then the researcher enrols his own face and seconds later unlocks it with a mask made of a 3D-printed visage constructed of stone powder, with 2D-printed eyes stuck on.



Credits: Rex, Daily Telegraph and Vocativ

# Building the Future of Identity

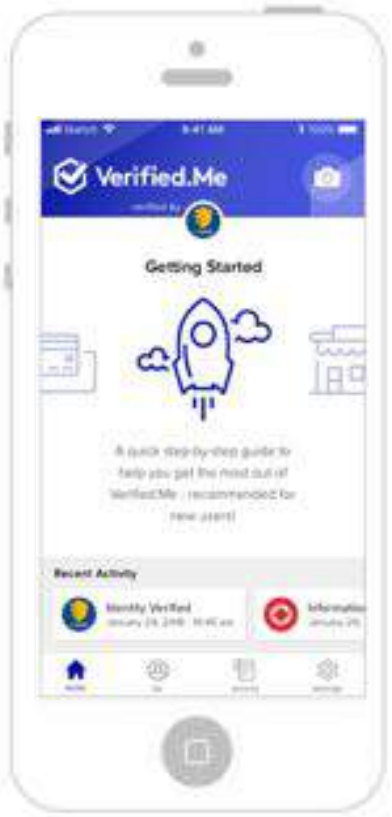
SECURE KEY

- Resiliency against denial of service attacks
- No honeypots of data
- Consumer centric with a strong consent model
- Separation of Authentication and Attestation Service Providers
- Triple blind privacy matter – where Data Providers and Data Consumers are blinded from each other and Broker Operator can not observe data
- Standard - OAuth 2.0 / OpenID Connect, NIST 800-63-3, GDPR

- **Needed Blockchain**

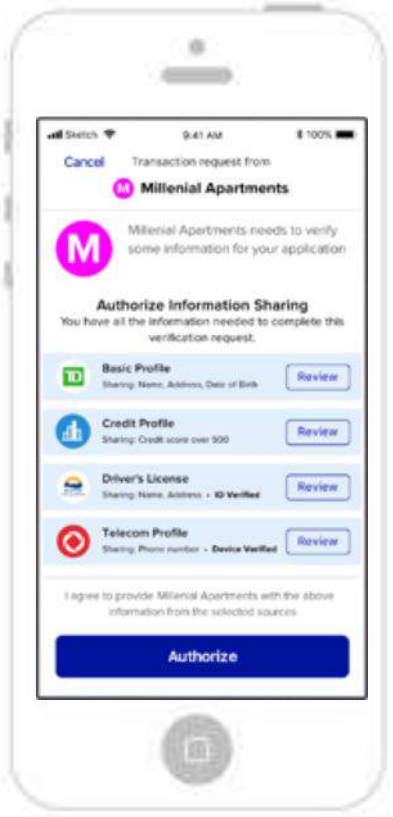
# Trusted Identity In Your Control

**A new service for customers to manage their digital identity**




Users connect with their bank and other trusted providers, layering information

**Enables safe and secure sharing of personal information**




Companies request information, users review and approve for real time delivery directly from trusted provider(s)

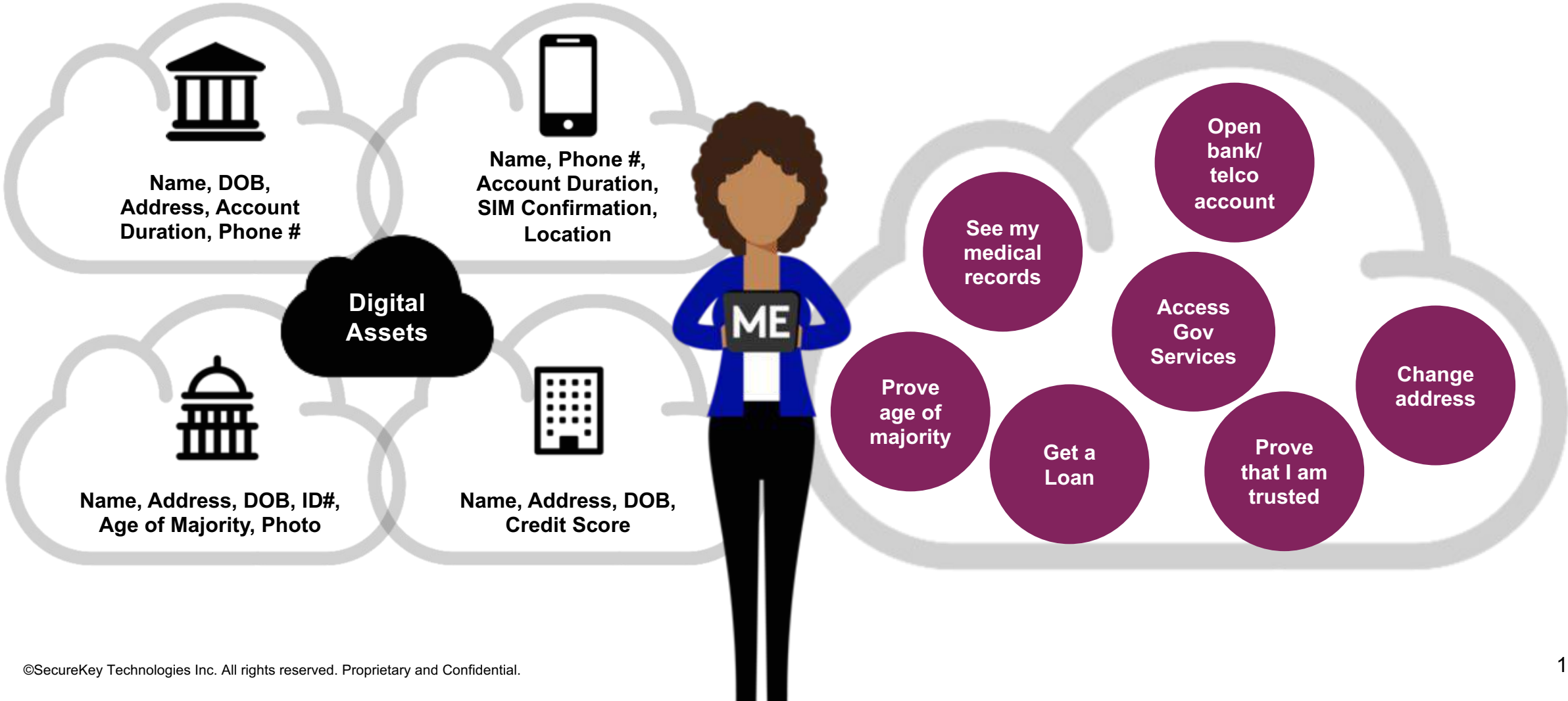
**High assurance by combining multiple factors, channels and ID claims**

**What I Know**

**What I Have**

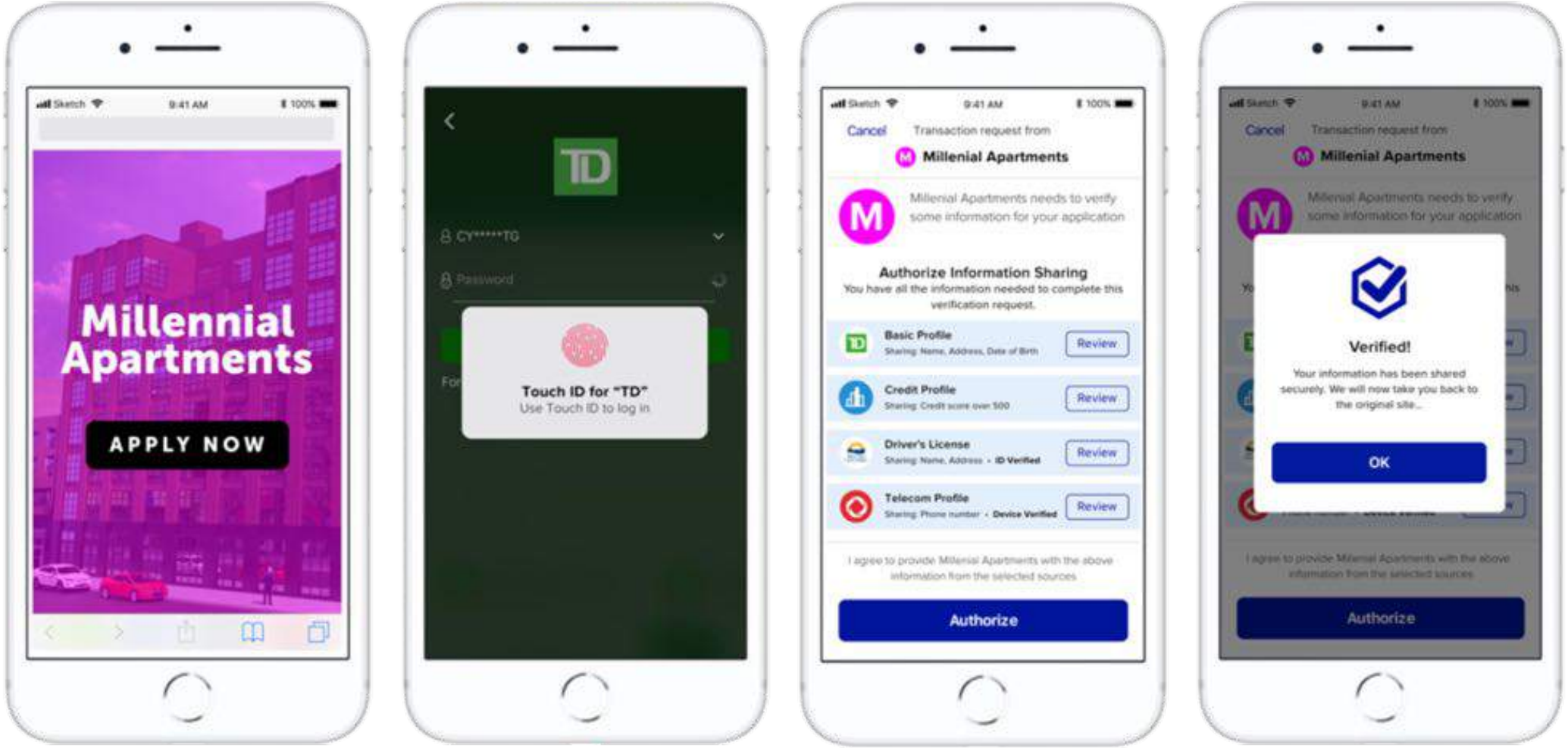
**What I Am**

# Digital Assets & Destinations

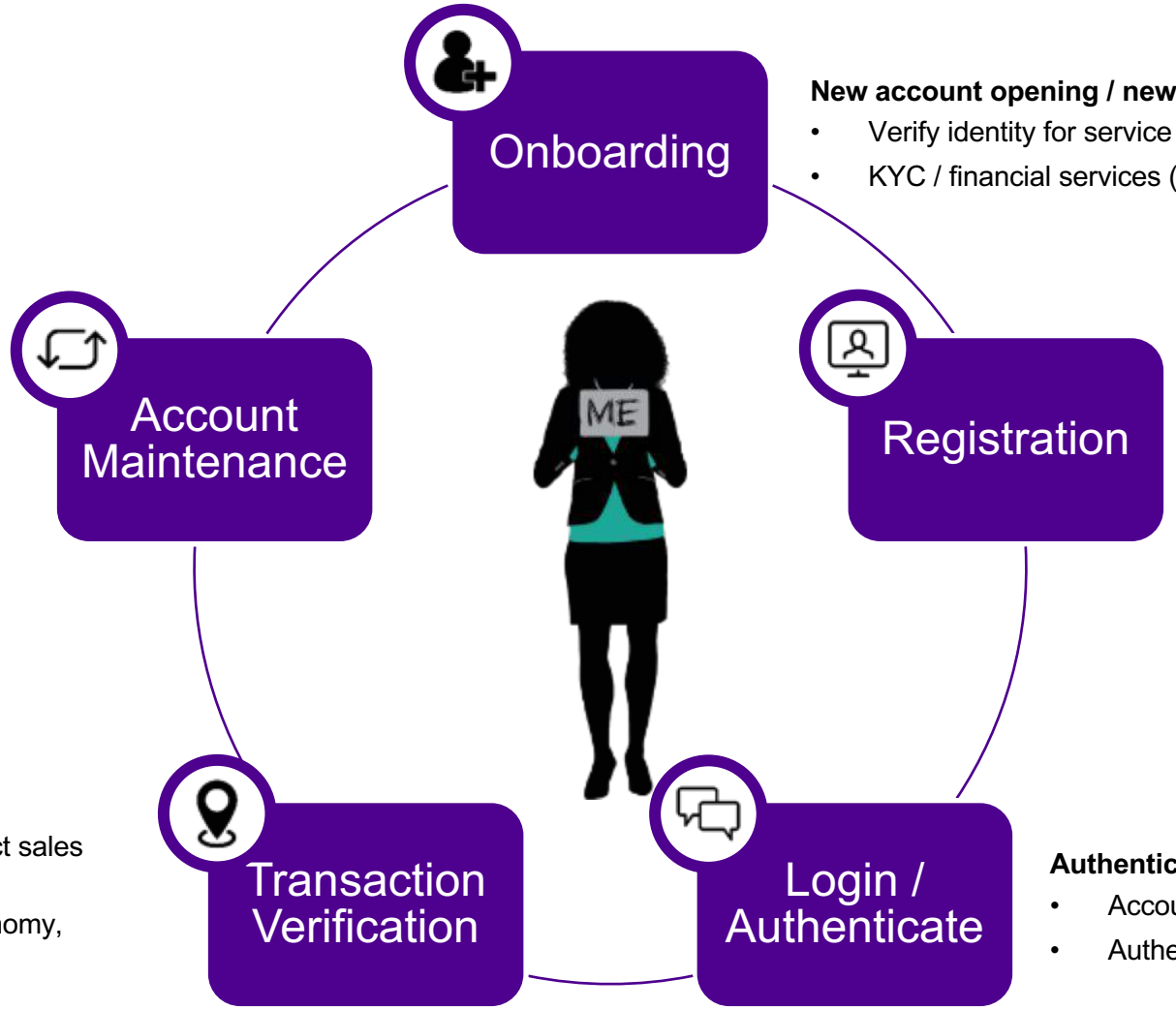


# DEMOS

# It Has to Work Online, In Person and on the phone



# Verified ID Helps Across the Customer Lifecycle




**New account opening / new user onboarding**

- Verify identity for service delivery
- KYC / financial services (accounts, loans, etc.)

**Self-serve account registration**

- Transition existing customers to online, self-serve channels

**Authenticate returning users**

- Account login or recovery
- Authenticate customers for support

**Validate user eligibility**

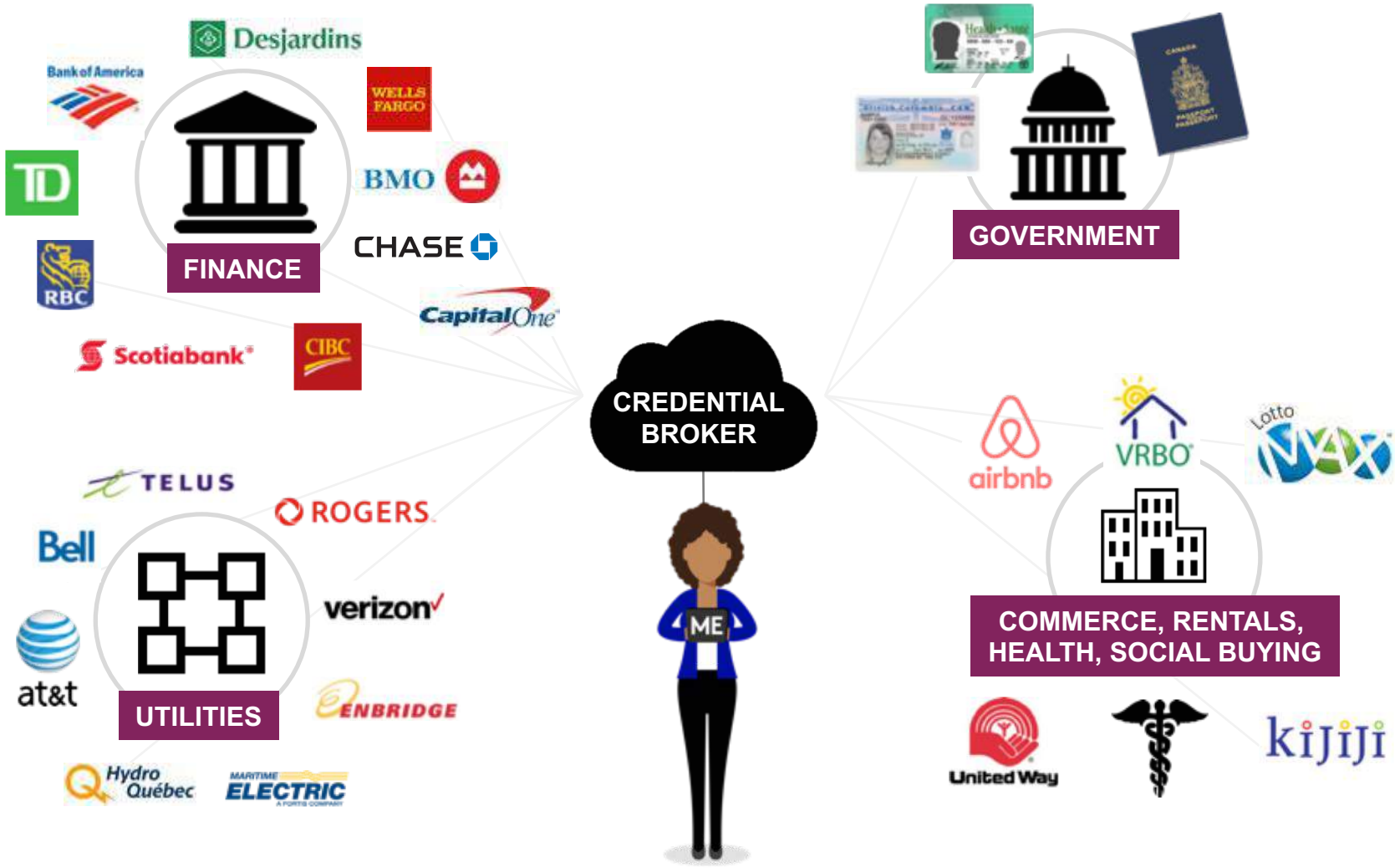
- Age and location verification for product sales (across channels)
- Background check for sharing/gig economy, tenant screening

**Update customer account information**

- Update address information and contact details
- Sign up for direct deposit

# Identity in the Present

## Central Credential Broker




**PROS**

- Easier to connect

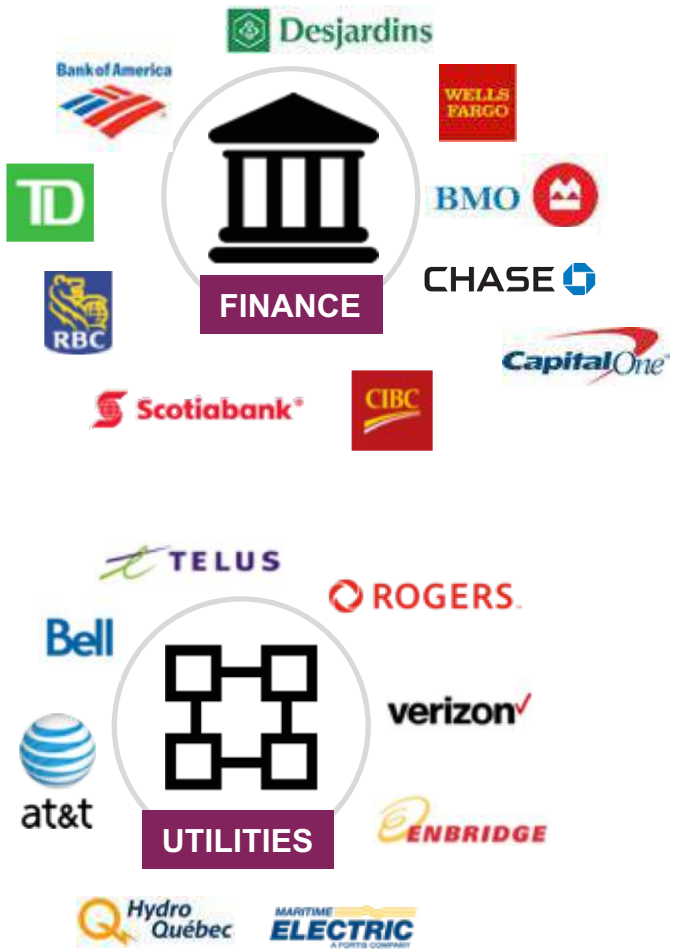
**CONS**

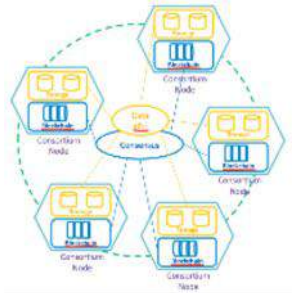
- Honest but Curious
- Single Point of Failure
- Often requires or builds honeypots of data (big fraud target)
- User Tracking
- Central mapping opens the data – relying on controls

# Identity in the Future

## Utilizing Strong Distributed Ledger Capabilities

SECURE KEY






**PROS**

- No Data visible to network operator
- No central database or honeypots
- No central point of failure
- Triple Blind – PRIVACY
- Cannot track user across relying parties
- Scalable
- Resiliency to DDOS

IBM HYPERLEDGER

# Hyperledger, a Linux Foundation Project

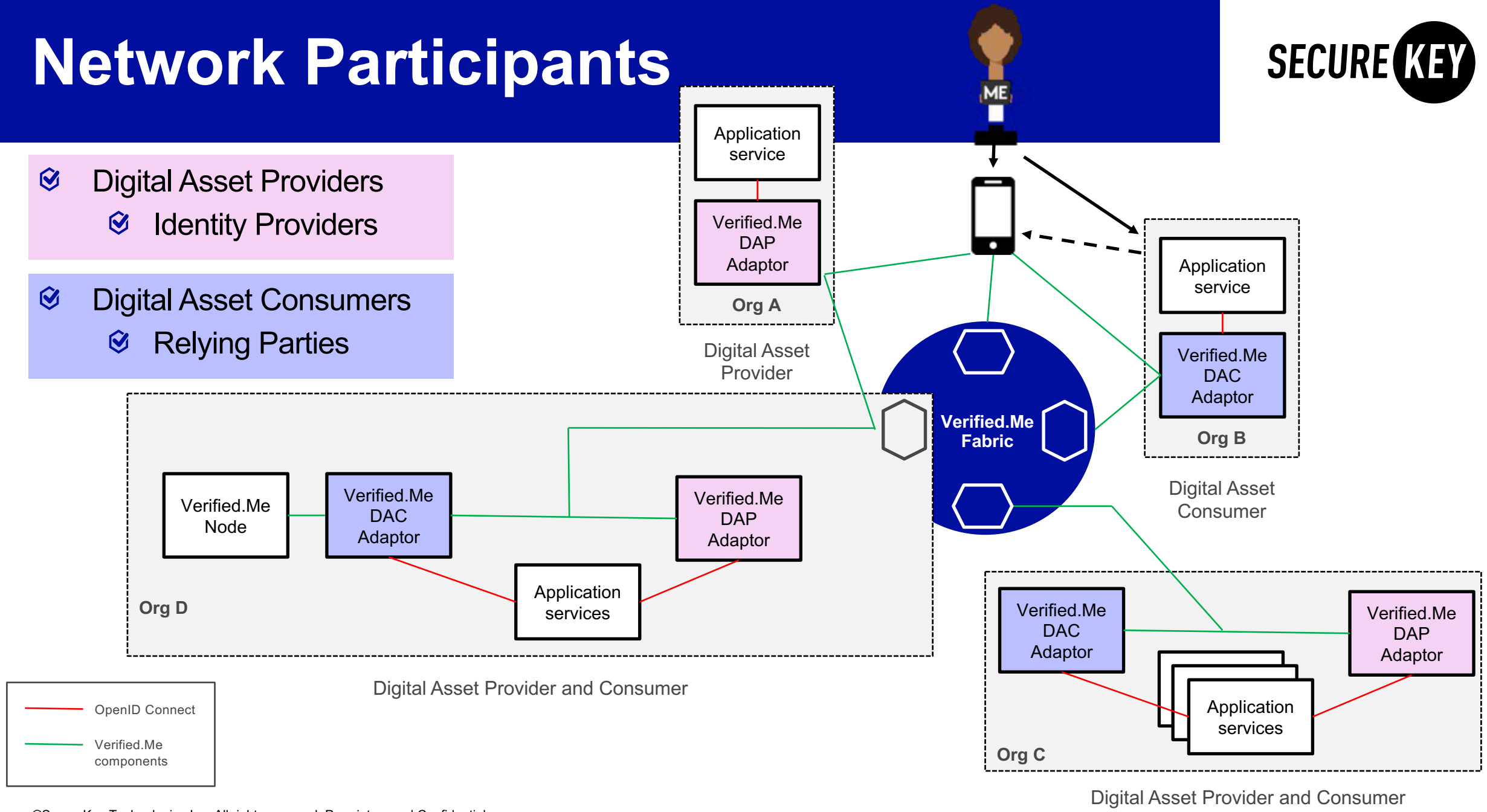
- Announced by The Linux Foundation on December 17, 2015 with 17 founders, now over 130 members
- Hyperledger is an open source and openly governed collaborative effort to advance cross-industry blockchain technologies for business, hosted by The Linux Foundation.
- Hyperledger Fabric is a blockchain framework implementation and one of the Hyperledger projects, intended as a foundation for developing applications/solutions with a modular architecture

**Enable adoption of shared ledger technology at a pace and depth not achievable by any one company or industry**

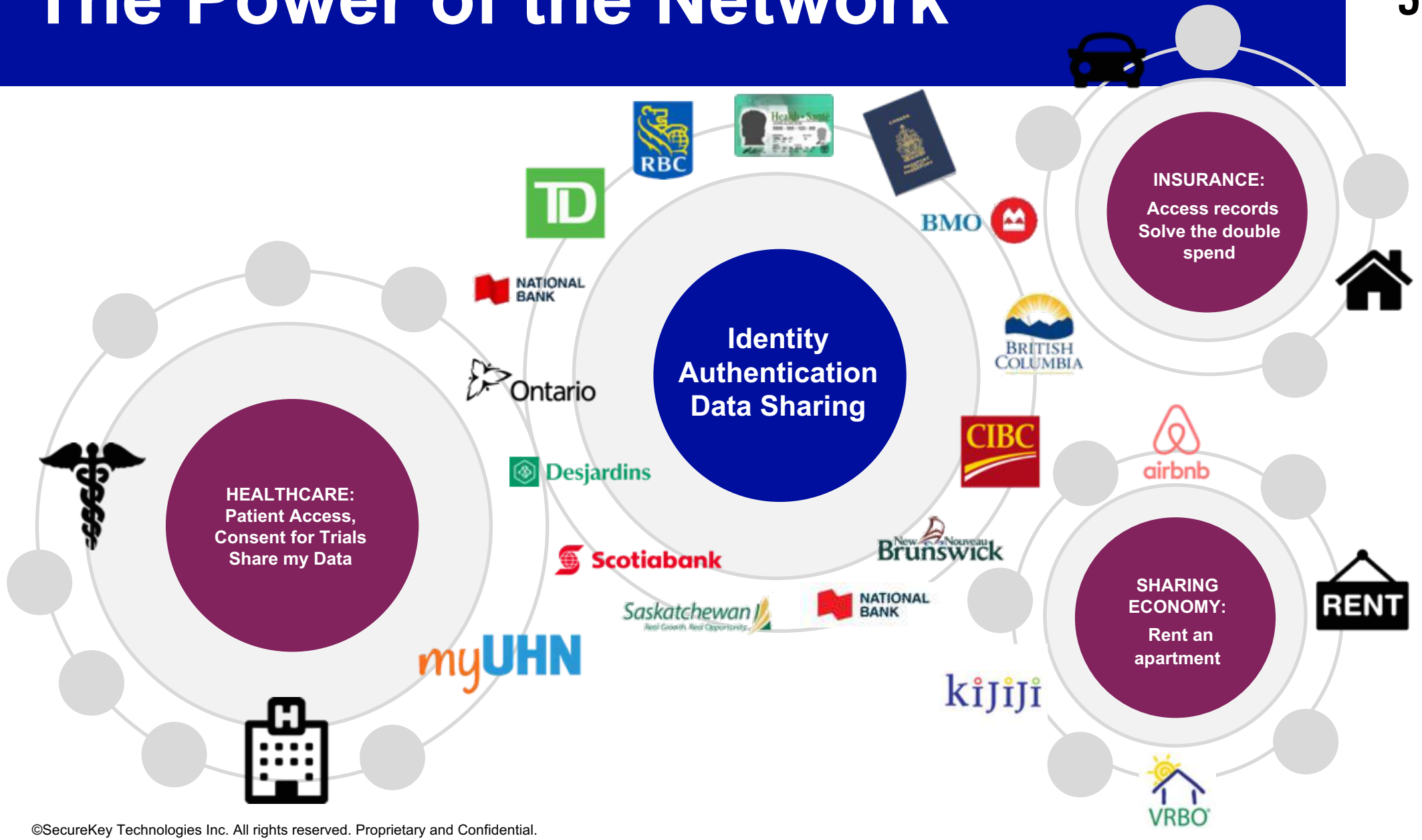

www.hyperledger.org

# Network Participants

- Digital Asset Providers
  - Identity Providers
- Digital Asset Consumers
  - Relying Parties



# The Power of the Network




Homeland Security

Science and Technology

Information in this presentation and/or video is based on research funded by the U.S. Department of Homeland Security Science & Technology Directorate (DHS S&T). Any opinions contained herein are those of the performer and do not necessarily reflect those of DHS S&T.

For more information, please contact:

Anil John

Program Manager
Cybersecurity R&D

anil.john@hq.dhs.gov

# THANK YOU!

**Dmitry Barinov | CTO**

SecureKey Technologies

Dmitry.Barinov@SecureKey.com

@ds_barinov

- This document contains information that is the property of SecureKey Technologies Inc. (SecureKey). All information contained in this document is confidential and proprietary to SecureKey.
- Please note that any disclosure, distribution, or copying of this document or the information in it is regulated by a confidentiality agreement with SecureKey. The document and information may not be copied, distributed or recorded in any electronic, physical, or other medium without the prior express written permission of SecureKey or otherwise in accordance with the confidentiality agreement.