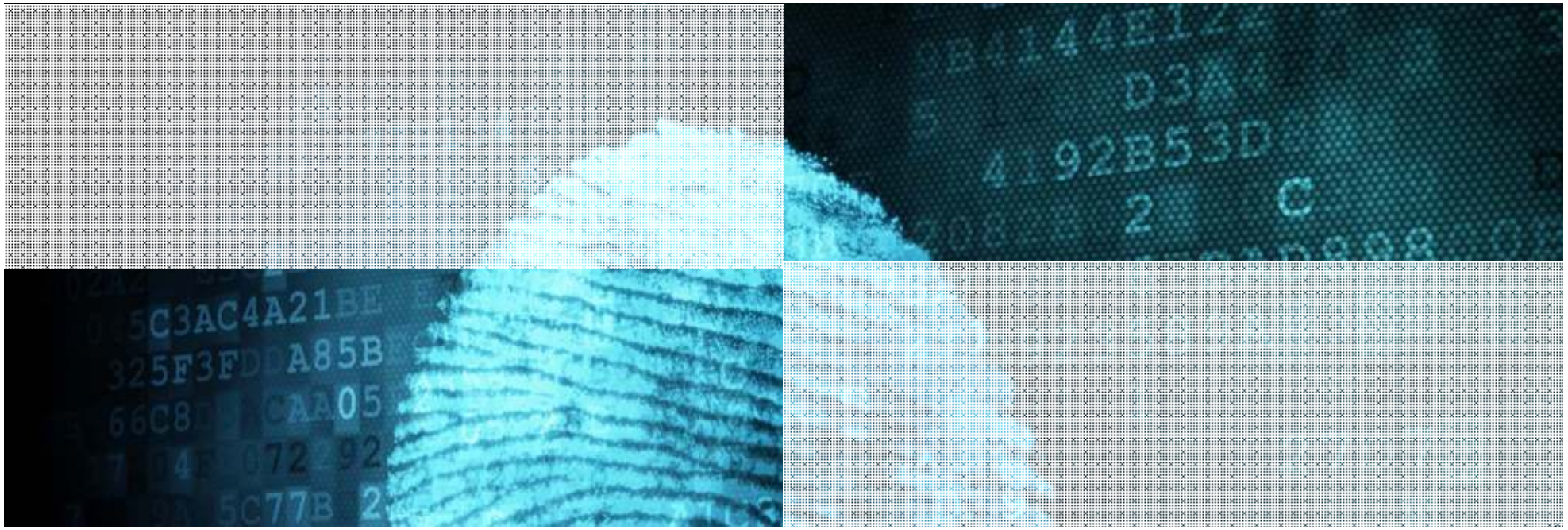
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

A Blueprint for Digital Identity

The Role of Financial Institutions in Building Digital Identity



An Industry Project of the Financial Services Community | Prepared in collaboration with Deloitte

Part of the Future of Financial Services Series • August 2016

Foreword

Consistent with the World Economic Forum's mission of applying a multi-stakeholder approach to address issues of global impact, the creation of this report involved extensive outreach and dialogue with the financial services community, innovation community, technology community, academia and the public sector. The dialogue included numerous interviews and interactive sessions to discuss the insights and opportunities for collaborative action.

We extend sincere thanks to the industry and subject matter experts who contributed their unique insights to this report. In particular, the members of the Project's Steering Committee and Working Group, who are introduced in the following pages, played an invaluable role as experts and patient mentors.

We are also very grateful for the generous commitment and support to Deloitte Consulting LLP in the U.S., an entity within the Deloitte[1] network, in its capacity as the official professional services advisor to the World Economic Forum for this project.

Contact

For feedback or questions, please contact:

R. Jesse McWaters, Lead Author
jesse.mcwaters@weforum.org
+1 (212) 703-6633

[1] Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Acknowledgements

Acknowledgements

Members of the Steering Committee

The following senior leaders of global financial institutions have provided guidance, oversight and thought leadership to the “Disruptive Innovation in Financial Services” project as its Steering Committee:

Bob Contri

Vice Chairman,
Deloitte & Touche LLP

David Craig

President, Risk and Financial,
Thomson Reuters

John Flint

Chief Executive Officer, Retail Banking and Wealth Management, *HSBC*

Kim Hammond

Chief Operating Officer,
Deutsche Bank

Jason Harris

Chief Executive Officer, International Property and Casualty, *XL Group*

Michael Harte

Chief Technology Officer and Chief Operations Officer, *Barclays*

Axel Lehmann

Chief Operating Officer,
UBS

Anju Patwardhan

Chief Innovation Officer,
Standard Chartered Bank

David Puth

Chief Executive Officer,
CLS Group

William Sheedy

Global Executive, Corporate Strategy, M&A, Government Relations, *Visa*

Dietter Wemmer

Chief Financial Officer,
Allianz

Acknowledgements

Members of the Working Group

The project team would also like to acknowledge the following executives of global financial institutions who helped define the project framework and shape strategic analyses as its Working Group:

Tom Brown

Partner,
Paul Hastings

Lena Mass-Cresnik, PhD

Head of Innovation, Strategic Product Management, *BlackRock*

Christof Edel

Global Head of Trading Strategy & Business Development, *Thomson Reuters*

Rob Galaski *(Project Advisor)*

Head of Financial Services,
Deloitte

Dorothy Hillenius

Director of Corporate Strategy,
ING

Marc Lien

Director of Innovation and Digital Development, *Lloyds Banking Group*

Matthew Levin

EVP and Head of Global Strategy,
Aon

Victor Matarranz

Director of Strategy & Chief of Staff to the CEO,
Santander

Neil Mumm

VP Corporate Strategy,
Visa

Max Neukirchen

Group Head of Strategy,
JP Morgan Chase

Christine O'Connell

Global Head of Strategy & Business Development, *Thomson Reuters*

Robert Palatnick

Managing Director and Chief Technology Architect, *DTCC*

Kosta Peric

Deputy Director Financial Services for the Poor, *Bill and Melinda Gates Foundation*

Justin Pinkham

SVP and Group Head, Payments Innovation,
MasterCard

Bob Reany

SVP and Group Head, Identity Solutions,
MasterCard

Peter Rutland

Senior Managing Director,
CVC Capital Partners

Nicolas de Skowronski

Chief of Staff,
Bank Julius Baer

Huw Van Steenis

Managing Director and Head of Financial Services Research, *Morgan Stanley*

Colin Teichholtz

Partner & Co-Head of Fixed Income Trading,
Pine River Capital

Fabien Vandenreydt

Head of Markets Management, Innotribe & the SWIFT Institute, *SWIFT*

Acknowledgements

List of subject matter experts (1 / 2)

In addition, the project team expresses its gratitude to the following subject matter experts who contributed their valuable perspectives through interviews and workshops (in alphabetical order):

Mukul Ahuja	Deloitte Canada
Christoph Albers	SWIFT
Alex Batlin	UBS
Eric Benz	Credits
Peter Berg	Visa
Vikram Bhat	Deloitte & Touche LLP
David Birch	Consult Hyperion
Francis Bouchard	Hamilton Place Strategies
Andre Boysen	SecureKey
David Brewer	Digital Catapult
Ben Brophy	ENTIQ
Tom Brown	Paul Hastings
Preston Byrne	Eris Industries
Claire Calmejane	Lloyds Banking Group
Alicia Carmona	Identity 2020
Nicolas Cary	Blockchain
Shawn Chance	Nymi
Emily Clayton	Bank of England
John Clippinger	MIT Media Lab
Jeff Coleman	Ledger Labs
Wayne Crombie	Citigroup
Malcolm Crompton	Information Integrity Solutions
Stephen Cross	Aon
Mark Davies	Avox Ltd.
Howard Davis	RBS
Nicolas de Skowronski	Julius Baer
Rachel Dixon	Digital Transformation Office of Australia
Ivan Djordjevic	Deloitte UK
Justin Dombrowski	Historiocity Tech
Jon Duffy	TradeMe
Carlo Duprel	Deloitte Tax & Consulting, Luxembourg
Andre Durand	Ping Identity
John Edge	Digital Stored Value Association
Anna Ewing	Nasdaq
Daniel Feichtinger	Digital Asset Holdings
Chris Ferguson	UK Cabinet Office
Jerry Fishenden	VoeTek
Marissa Flowerday	TradeMe
Conan French	IIF
Emilio Garcia	Santander
Joe Guastella	Deloitte Consulting LLP
Alka Gupta	Global ID
Aran Hamilton	DIACC
Jonathan Hardinges	Thomson Reuters
Adrienne Harris	National Economic Council, The White House
Jonathan Hayes	Julius Baer
Dorothy Hillenius	ING
Bill Hodash	DTCC
Rainer Hoerbe	The Kantara Initiative
Chuck Hounsell	TD Canada
Arne Vidar Huag	Signicat
Afsar Hussain	GSMA
Marta Ienco	GSMA
Raj Iyer	BNY Mellon
Natasha Jackson	GSMA
Charlotte Jacoby	Agency for Digitization, Ministry of Finance, Denmark
Hyder Jaffrey	UBS
Andrew Johnston	TELUS
Tanis Jorge	Trulioo
Sean Kevelighan	Zurich Insurance Group
Alim Khalique	Bank of America Merrill Lynch
Hwan Kim	Deloitte Canada
Dan Kimerling	Standard Treasury
Philipp Kroemer	Commerzbank AG
Jaap Kuipers	Kantara Initiative
Jo Lambert	Paypal
Ian Lee	Citi
Chris Locke	Caribou Digital
Joseph Lubin	Consensys
Adam Ludwin	Chain
Christian Lundkvist	Consensys

Acknowledgements

List of subject matter experts (2 / 2)

In addition, the project team expresses its gratitude to the following subject matter experts who contributed their valuable perspectives through interviews and workshops (in alphabetical order):

Joanna Marathakis	Deloitte Transactions and Business Analytics LLP
Stephen Marshall	Deloitte UK
Simon Martin	LeapFrog Investments
Todd McDonald	R3CEV
Morgan McKenney	Citigroup
Adel Melek	Deloitte Canada
Pat Meredith	Canadian Payments Taskforce
Paul Morgenthaler	Commerzbank
Renny Narvaez	BNY Mellon
Eddie Neistat	AlixPartners
Nina Nieuwoudt	Mastercard
Pascal Nizri	Chekk
Robert Palatnick	DTCC
Cheryl Parker Rose	CFPB
Justin Pinkham	MasterCard
Rick Porter	Deloitte & Touche LLP
Reinhard Posch	Austrian Federal Government
Dan Quan	CFPB
Rhomaios Ram	Deutsche Bank
Kai Rannenberg	Goethe University
Bob Reany	Mastercard
David Richards	DIACC
Pierre Roberge	Digital and Payment Innovation Consultant
Andre Romanovskiy	Deloitte Canada
Andrew Rudd	AssureUK
Peter Rutland	CVC Capital Partners
Wiebe Ruttenberg	European Central Bank
Joel Sacmar	Daon
Jean-Louis Schiltz	Schiltz & Schiltz
Charles Schwarz	Barclays
Rocky Scopelliti	Telstra
Amy Scott	Identity2020
John Scott	2Keys Security Solutions
Anton Semenov	Commerzbank
Beth Shah	Digital Asset Holdings
Rajesh Shenoy	Citi
Nick Smaling	Deloitte Netherlands
Stan Stalnaker	HubID
Matthew Stauffer	Clarient Entity Hub
Gavin Steele	Lloyd's of London
Ashley Stevenson	ForgeRock
Matt Stroud	Digital Catapult
Paul Szurek	Blockchain
Pavlo Tanasyuk	BlockVerify
Marc Taverner	BitFury
Simon Taylor	Barclays
Adizah Tejani	Level39
Kenneth Tessem	Finansiell ID-Teknik BID AB
Don Thibeau	Open Identity Exchange (OIX)
Michael Turner	PERC
Keith Uber	GlobalSign
Eric Van der Kleij	Level39
Huw van Steenis	Morgan Stanley
Aneesh Varma	Aire.io
Ivan Vatchkov	Algebris Investments
Roy Vella	Vella Ventures Ltd.
Helene Vigue	GSMA
Franziska von Arnim	Deutsche Bank
Patrick Walker	PERC
Colin Wallis	Kantara Initiative
Peter Watkins	Government of British Columbia
Derek White	Barclays
Conor White	Daon
Greg Williamson	MasterCard
Gregory Williamson	MasterCard
Stephan Wolf	GLEIF
Kevin Young	Deloitte Canada
Fei Zhang	Allianz
Tom Zschach	CLS Bank

Acknowledgements

Project Team and Additional Thanks

Project Team

The “Disruptive Innovation in Financial Services” project team includes the following individuals:

WORLD ECONOMIC FORUM PROJECT TEAM

Jesse McWaters
Project Lead, Disruptive Innovation in Financial Services

Giancarlo Bruno
Senior Director, Head of Financial Services Industries

Michael Drexler
Senior Director, Head of Investors Industries

PROFESSIONAL SERVICES SUPPORT FROM DELOITTE

Rob Galaski
Project Advisor, Deloitte

Christine Robson
Lead Author, Deloitte

Additional Thanks

The project team expresses its gratitude to the following individuals for their contribution and support throughout the project (in alphabetical order):

Faiza Harji

Alex Rinaldi

Sabrina Sdao

And to:

The Deloitte Greenhouse (Event Facilitation & Location Services)

Level 39 (Location Services)

The Value Web (Event Facilitation)

Executive Summary

The Blueprint for Digital Identity project is the most recent phase of the Forum's ongoing Disruptive Innovation in Financial Services work

2015

THE FUTURE OF FINANCIAL SERVICES

The Future of Financial Services project explored the landscape of disruptive innovations in financial services, provided the first consolidated taxonomy for these disruptions, and explored their potential impacts on the structure of the industry

2016

BEYOND THE FUTURE OF FINANCIAL SERVICES

This phase of the disruptive innovation work explores two topics with key potential as foundational enablers of future disruption

A Blueprint for Digital Identity: The role of Financial Institutions in building Digital Identity

This project explores the potential for digital identity in financial services and beyond and lays out a blueprint for the implementation of effective digital identity systems

The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services

This project explores the potential for distributed ledger technology to transform the infrastructure of the financial services industry

The mandate of this project was to explore digital identity and understand the role that Financial Institutions should play in building a global standard for digital identity

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

PROJECT CONTEXT

Identity is a critical topic in Financial Services today. Current identity systems are limiting Fintech innovation and well as secure and efficient service delivery in Financial Services and society more broadly. Digital identity is widely recognized as the next step in identity systems. However, while many efforts are underway to solve parts of the identity challenge and create true digital identity, there is a need for a concerted and coordinated effort to build a truly transformational digital identity system.

This document is intended as a guide for Chief Strategy Officers of Financial Institutions as well as policy makers who are interested in the topic of identity and want to understand the digital identity and their own potential role in the creation of robust digital identity systems.

PROJECT SCOPE

The mandate of this project was to explore identity and its importance in Fintech, Financial Services and in developed societies broadly, the topic of digital identity, and provide a landscape scan of current efforts to build digital identity solutions.

This report will discuss different structures for identity systems and discuss which configurations are best suited to solve different problems, and provide a perspective on the role of Financial Institutions in building digital identity systems.

This report will not focus on the creation of standards around identity; much valuable work has already been done in this space and current developments such as the publication of the European Union eIDAS Regulation are moving the conversation on this front. Nor will it discuss technology solutions. Rather, it will attempt to provide clarity and direction around the structure of identity and provide a call to action for Financial Institutions to move against the identity challenge.

Over 12 months of research we engaged with subject matter experts through interviews and multi-stakeholder workshops

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Industry Leaders

Guidance and thought leadership from **12 C-suite executives and 24 strategy officers** of global financial institutions

Subject Matter Experts

In-person and phone interviews with **100+ subject matter and industry experts**

Global Workshops

Four multi-stakeholder workshops at global financial hubs with 200+ total participants including industry leaders, innovators, subject matter experts, and regulators

Singapore	New York, USA	London, UK	Davos, Switzerland
Oct. 2015	Nov. 2015	Dec. 2016	Jan. 2016

This report synthesizes our findings and presents a Point of View on the role that we see for Financial Institutions in digital identity

PROJECT OUTCOMES

Our Perspective: The Role of Financial Institutions in Digital Identity

How should Financial Institutions engage with digital identity? What role can they play in the development of digital identity solutions?

1	**Introduction** What is the global identity challenge, and what problems does it pose for Financial Institutions?
2	**Digital Identity Primer** What is the purpose of identity systems, and why is digital identity the solution to the global identity challenge?
3	**The Landscape of Digital Identity** What do efforts to build digital identity systems look like globally?
4	**The Right Solution to the Right Problem** How should digital identity systems be constructed to serve different needs?
5	**Benefits of Digital Identity** Who stands to benefit from the introduction of digital identity systems?
6	**Implementation** How do you reach a global digital identity solution?

The Role of Financial Institutions in Digital Identity

Current identity systems place major limitations on Fintech innovation

Lack of digital identity limits the development and delivery of efficient, secure, digital-based Fintech offerings

Identity is currently a critical pain point for Fintech innovators. Many of these innovators are trying to deliver pure digital offerings, but the process of identifying users consistently forces them to use physical channels. These Fintech innovators now see the development of a new generation of digital identity systems as being crucial to continuing innovation and delivering efficient, secure, digital-based Fintech offerings.

Examples

Payments

Payments require validation of ACH information, meaning that digital payments innovators must either require users to provide identity information through pseudo-digital channels (such as by photographing their driver's license) or act as platforms on top of established Financial Institutions and rely on their KYC processes

Loans

Evaluating customer risk and issuing loans requires validation of basic customer information, requiring innovators to gather information from users, again through pseudo-digital channels such as photographing existing ID or gathering trusted information from an existing source, and therefore decentralizing a central piece of the product offering

Digital identity is a critical enabler of activity inside Financial Services broadly

Digital identity would allow FIs to perform critical activities with increased accuracy over that afforded by physical identity, and to streamline and partially or fully automate many processes

Identity is also central to the broader financial services industry, enabling delivery of basic financial products ands services. Reliance on physical identity protocols introduces inefficiency and error to these processes. Digital identity has great potential to improve core financial services processes and open up new opportunities.

Examples

Operational decisions

Traditional FS offerings such as insurance and credit and well as customer experience such as contact centers and collections rely on accurate and detailed knowledge of the customer

Regulatory compliance

FIs are required to comply with strict regulation on identifying their customers and are liable for mistakes and inaccuracies

Customer experience and product delivery

Improved knowledge of customer preferences and habits can help FIs deliver radically better customer experience (e.g., tailor authentication requirements based on behaviour)

The relevance of digital identity stretches beyond Financial Services to society as a whole

Identity enables many societal transactions, making strong identity systems critical to the function of society as a whole

Physical identity systems currently put users at risk due to overexposure of information and the high risk of information loss or theft; they also put society at risk due to the potential for identity theft, allowing illicit actors to access public and private services. Digital identity would streamline and re-risk completion of these public and private transactions.

PUBLIC TRANSACTIONS

Entities are required to prove their identities or certain attributes to demonstrate their eligibility for public services

Examples

- *Access to social assistance (e.g., old age security, unemployment insurance)*
- *Access to education*
- *Access to healthcare*
- *Access to civic structures (e.g., voting)*

PRIVATE TRANSACTIONS

Entities are often required to prove their identities or certain attributes to participate in private transactions

Examples

- *Many basic merchant transactions (e.g., buying alcohol)*
- *Large private provider transactions (e.g., renting an apartment, buying a car)*

The need for digital identity is becoming increasingly pressing

Five key trends are increasingly the need for efficient and effective identity systems:

1

Increasing transaction volumes
The number of identity-dependent transactions is growing through increased use of the digital channel and increasing connectivity between entities

2

Increasing transaction complexity
Transactions increasingly involve very disparate entities without previously established relationships (e.g., customers and businesses transacting cross-border)

3

Rising customer expectations
Customers expect seamless, omni-channel service delivery and will migrate to services that offer the best customer experience

4

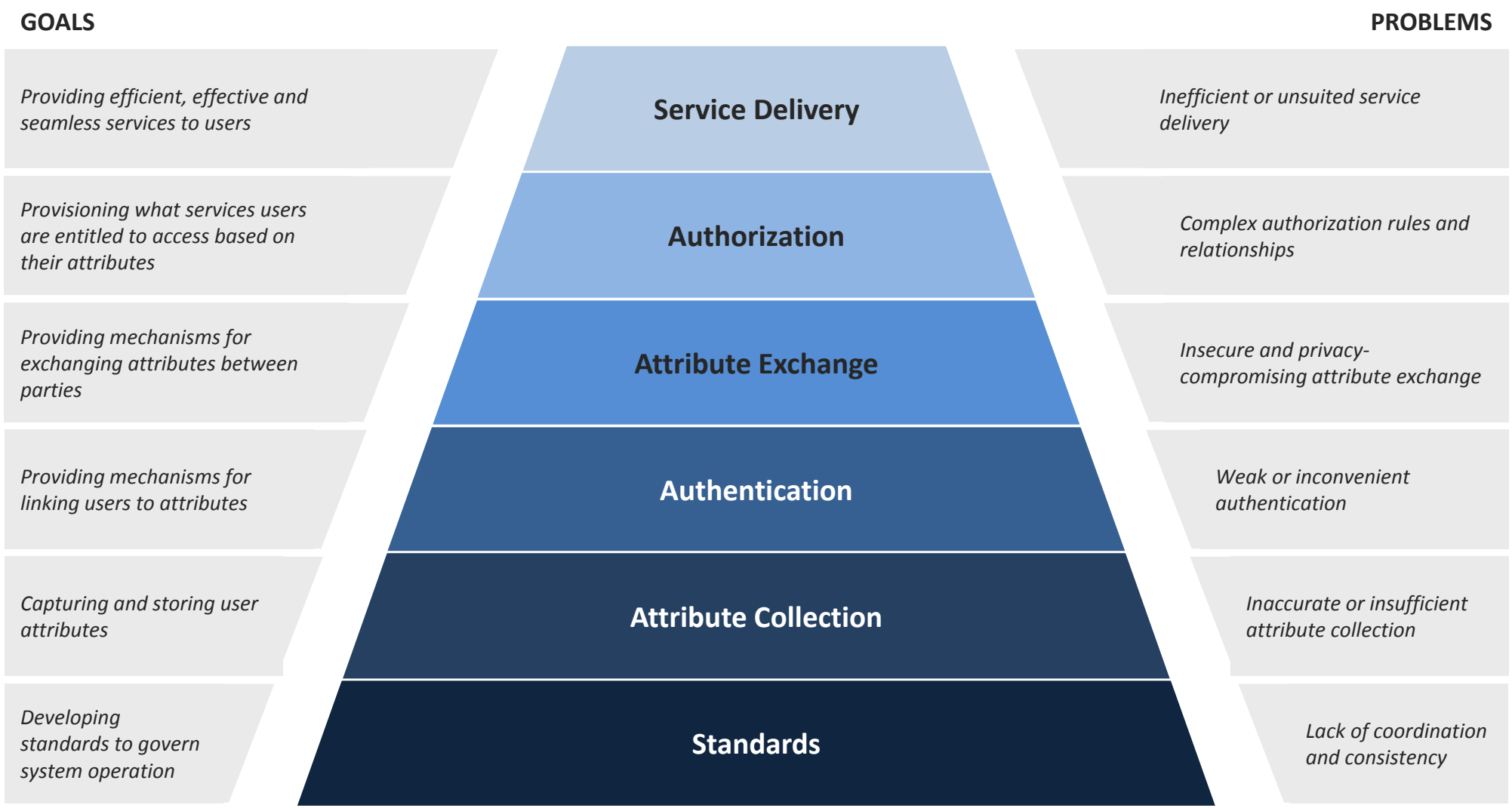
More stringent regulatory requirements
Regulators are demanding increased transparency around transactions, meaning that FIs require greater granularity and accuracy in the identity information that they capture and are increasingly being held liable for inaccurate or missing identity information

5

Increasing speed of financial / reputational damage
Bad actors in financial systems are increasing sophisticated in the technology and tools that they use to conduct illicit activity, increasing their ability to quickly cause financial and reputational damage by exploiting weak identity systems

However, identity is a multi-layered problem making the creation of digital identity systems complex

Each layer of identity of serves a different purpose, and suffers from a distinct set of problems in today's identity landscape



There are currently many distinct gaps in the digital identity landscape

1. Confusing authentication with identity

Many efforts today focus on authentication as a solution to the identity challenge without addressing the strength of the underlying attribute collection and authorization processes

- *Authentication technology solutions, while valuable, rely on preexisting onboarding and attribute collection processes*
- *Authentication solutions provided by global technology platforms are convenient for users but do not provide security or verification of the identity behind an account or username*

2. Enabling transaction completion rather than user activity

Many solutions are driven by the goals and perspectives of a single organization and therefore are designed to serve the needs of particular transactions rather the broader needs of users

- *eGovernment solutions are intended to make government service delivery to users more efficient, and do not enable further transactions in which users might want to participate*
- *Transaction-focussed solutions result in the repeated collection of 'tombstone' data rather than effective collection of user-centric and risk-relevant data such as transaction habits*

3. Building consensus rather than driving action

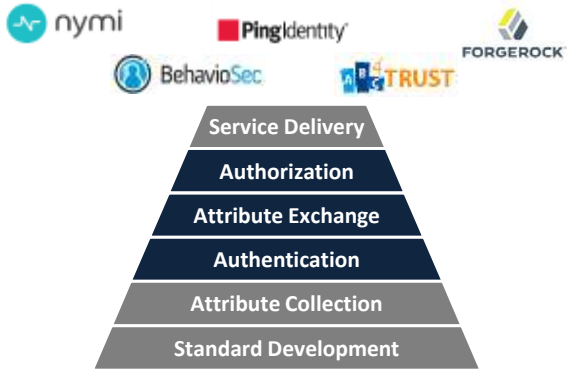
Many efforts focus on building agreement around standards and processes rather than creating a full identity solution and therefore do not result in private sector-implementable solutions

- *Utilities and standards organizations are focussed on creating consensus and a standardized view of data, rather than providing a full identity solution*
- *Multi-governmental efforts have considerable scale but are mainly focussed at the regulatory level, and do not offer a commercially viable solutions*

These gaps are a result of the crowded digital identity landscape, with many different entities building solutions

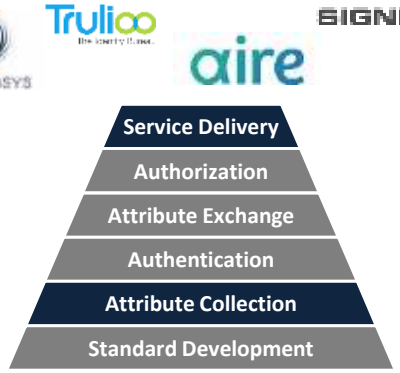
Technology solution providers

Technology solution providers focus on point solutions for authentication, attribute exchange or identity management for enterprises



Private Service Providers

Private service providers focus on collecting the attributes they themselves need to provide specific services to users

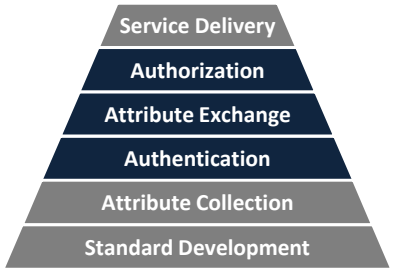


Global technology companies

Global technology companies act as platforms to authenticate users to a wide variety of other service providers

Industry Bodies

Industry bodies focus on standardizing and centralizing the collection of attributes within that specific industry



Governments

Governments focus on the provision of identity to their citizens, and providing citizens with services based on these attributes

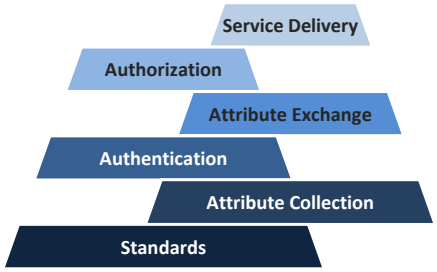
Standards Organizations

Standards organizations focus on frameworks and guidance for developing identity systems

There is an opening for new digital identity systems that can deliver scope and scale

While many ongoing efforts, such as new authentication solutions, are critical to building digital identity, there is a core need for a strong system will enable effective action against each layer of the stack

The entire stack does not need to be provided by a single entity – some components may be modular – but the entire stack must be effective and integrated to provide digital identity systems that have certain critical features



Critical characteristics of a strong identity system

1. **Operationally effective**
   The system allows digital transactions to be completed conveniently and effectively

2. **Scope & scale**
   The system enables large volumes of transactions through provision of transaction-critical attributes and connecting large numbers of users with important and frequently used service providers

3. **Security**
   The system prevents user information from being overexposed, lost or stolen

4. **User control & privacy**
   The system allows users to determine where their information is held and when it is shared or exposed

5. **Viability**
   The system delivers value to all stakeholders, creating broad support and uptake and making it a commercially viable system

Financial Institutions are well positioned to drive the creation of digital identity systems

Financial institutions are exceptionally well positioned to drive identity systems that fill the gaps left by current efforts

	STRUCTURAL
1	FIs already act as **stores of customer attributes** for their own commercial purposes, and therefore are positioned to act as identity providers without extensive incremental effort
2	FIs are one of very few types of institutions that can **verify user information**; they already perform this function for commercial and regulatory purposes
3	FIs are **incentivized to collect accurate user information** for their own commercial purposes
4	FIs have **proven executional ability** to develop new systems and standards (e.g., Interac) that have been widely adopted and effectively used within the private sector
5	The FS industry has near-complete **coverage of users** (people, legal entities, and assets) in developed economies
6	Global FIs have interconnected **operations across multiple jurisdictions**, giving them a structural advantage in enabling cross-jurisdictional identity transactions and systems

	POSITIONING
1	FI operations and use of customer data are **rigorously regulated**
2	FIs act as **established intermediaries** in many transactions and are therefore well positioned to act as identity intermediaries
3	FIs are typically **trusted by consumers** beyond other institutions to be safe repositories of information and assets

There is a strong business case for Financial Institutions to lead the development of digital identity systems

FIs could derive substantial benefit from investing in the development of digital identity solutions. We have categorized these benefits into three categories: efficiency / cost avoidance, new revenue opportunities & brand enhancement, and transformational future state opportunities

Efficiency / Cost Avoidance

Opportunities to streamline current processes, increase automation, and reduce error and human intervention

New Revenue Opportunities

Opportunities to create new revenue streams from new products and services, and to increase the positive recognition of the brand

Transformational Future State Opportunities

Opportunities to stretch outside of core business and capabilities to create transformational new business models and reach new customers

Financial Institutions could benefit from basic efficiency improvements and cost avoidance…

Efficiency / Cost Avoidance

Process streamlining & automation
Streamline and improve onboarding and compliance processes through access to a reliable and consolidated digital view of user attributes, minimizing RFIs and information remediation due to inaccuracy and human error

Improved service delivery
Provide increasingly tailored products and services to customers by leveraging non-traditional attributes
Improve process efficiency and increase STP by automating processes through use of standardized, reliable digital data

Improved customer experience
Improve customer experience by leveraging a variety of user attributes to better understanding the customer's needs and preferences

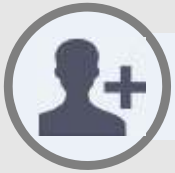
Improved risk assessment & scoring
Improve risk assessment and reduce fraud by creating more holistic and accurate customer risk profiles to inform suspicious transaction monitoring, insurance payouts, and provision of credit- and risk-based products

Develop new revenue streams…

New Revenue Opportunities

New financial products & services
Offer new products and services based on increased knowledge of customers (e.g., extended financial advisory, new insurance products such as insurance on fractionally owned assets and behaviour-based insurance)

Identity-as-a-service
Offer identity as a service to relying parties who cannot or do not wish to store customer information



Identity-only customers
Offer identity as a separate, fee-based service for individuals who do not otherwise transact with that FI

… and stretch beyond current business and markets to fundamentally transform their businesses

Transformational Future State Opportunities

Allocation of liability
Shift the liability for incorrect information, and the outcomes of holding this information, from Financial Institutions to other entities in the network (e.g., users through approval and consent requirements)

Trust brokerage
Act as a 'broker of trust' in previously trustless interactions between disparate parties in multiple industries, expanding the reach of FIs beyond the FS industry and reaching new profit pools

Disruption of the credit bureau model
Evaluate customer creditworthiness based on accurate identity data including preferences and financial history rather than relying on third parties and the mining of multiple different data sources

Refocussing around the customer
Refocus business around customer service, assisting with day-to-day decisioning and blurring the lines between financial and non-financial advisory

Public sector partnerships
Become the trusted identity provider of the public sector, assisting with social services and civic requirements such as tax filing

We are calling on FIs to champion the development of digital identity systems

FIs should champion efforts to build digital identity systems, driving the building and implementation of identity platforms through the creation of minimum viable digital identity systems

Requirements of a minimum viable identity system

1	**Identity provision** Identity provider(s) that hold trusted information and have coverage over a critical mass of users within their target area, and can therefore serve a large number of users and transactions
2	**High-transaction volume attributes** Secure storage of verified attributes that are required for common transactions (inherent attributes such as name, date of birth, nationality, national identifier number, and some assigned attributes such as address)
3	**Relying party adoption** Involvement of relying parties that offer important and frequently used user-facing services
4	**Technology platform** A technology platform that enables secure attribute exchange between identity providers and relying parties with a convenient user consent mechanism (e.g., operates on mobile and desktop)
5	**System standards** Supervisory & liability standards that guide operation and use of user information in the system and provide liability and user recourse
6	**Legal & regulatory acceptance** Legal & regulatory acceptance for using third-party verified information, attribute exchange and external use of user information

FIs could take several different approaches to creating identity systems

There are different configuration options for the development of digital identity systems, each with advantages and drawbacks

Single-Institution

Global institutions could create internal systems that stretch across the jurisdictions in which they operate

This would enable quick implementation but a single institution would likely have difficulty in gaining a critical mass of users, limiting its ability to drive system adoption and integration of relying parties

Consortium

Consortiums of financial institutions could form networks that cover large, contained oligopoly economies (such as Canada or Australia)

A consortium requires a high degree of collaboration among parties but is an effective method of getting complete coverage over a user group

Consortiums are well suited to provide identity for individuals as data storage is not centralized, increasing privacy and system resilience

Utility

Financial Institutions could create industry utilities to deliver identity services across the industry

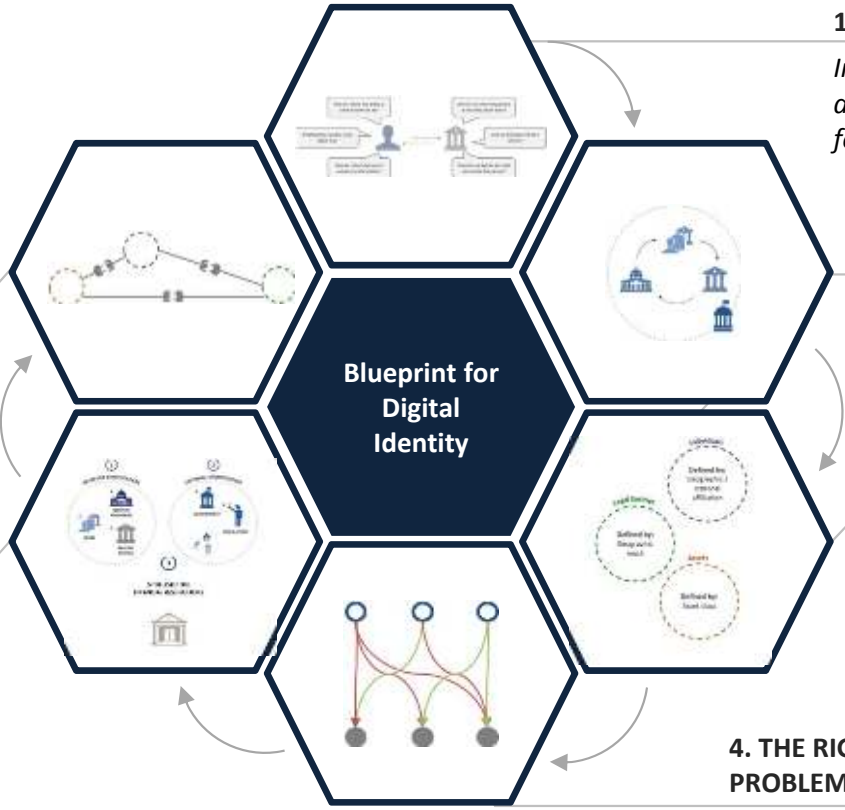
This model is effective in creating standardization and broad coverage, but implementation may be difficult due to the involvement of many different stakeholders

Utilities are a good model for legal entity and asset identity because they provide a standardized view and golden record of information

This report will provide guidance on constructing effective and robust digital identity systems while avoiding implementation pitfalls

Implementation of identity systems is extremely sensitive and therefore easy to get wrong; situational, operational and cultural factors all have important implications for identity systems, and implementation or operational failure has extremely negative consequences for both the drivers of identity system (e.g., wasted resources) and for users (e.g., data breaches).

We have studied the landscape of identity providers to understand what efforts are ongoing and which system models are best suited to different situations and to provide recommendations on system configuration and implementation.



1. INTRODUCTION

Introduces the global identity challenge and how problems with identity manifest for Financial Institutions

2. DIGITAL IDENTITY PRIMER

Summarizes key digital identity concepts

3. THE LANDSCAPE OF DIGITAL IDENTITY SYSTEMS

Describes the landscape of digital identity solutions and introduces a set of archetypes that represent the existing set of solutions

4. THE RIGHT SOLUTION TO THE RIGHT PROBLEM

Discusses how identity solutions should be configured for success

5. BENEFITS OF DIGITAL IDENTITY

Introduces the stakeholders that are involved in a digital identity network, and the types of benefits each stakeholder may derive

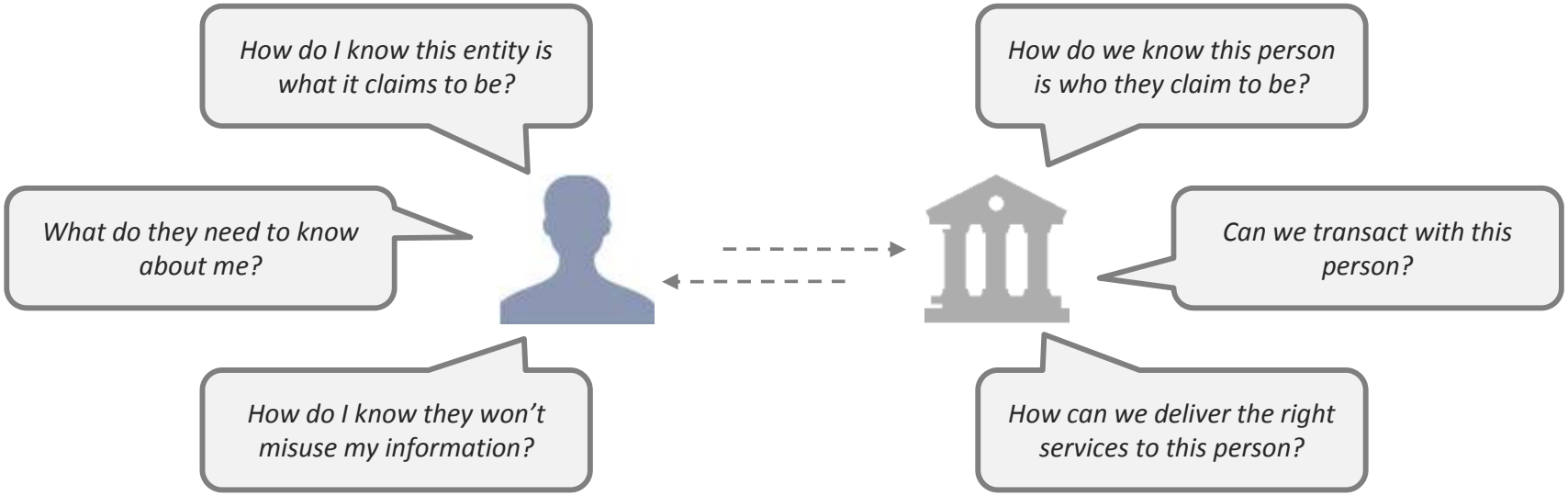
6. IMPLEMENTATION, INTERCONNECTION & CALL TO ACTION

Highlights the next steps and key stakeholders that must be involved to successfully implement a digital identity network

The Global Identity Challenge

Identity is critical to today's society

Identity is foundational to many of the transactions that occur in today's society. In any exchange with requirements about the transacting parties – they must be a certain age or reside in a certain jurisdiction – structures must be in place that allow entities to determine certain information about their counterparty, and to have confidence that the information is true.



THE ROLE OF IDENTITY IN TRANSACTIONS

Many transactions do not require identity. Some, such a crime reporting, may in fact require anonymity. However, many transactions do require identity: to determine if the necessary conditions for the transaction to occur exist, to establish a relationship for repeated transactions, or to tailor delivery of products and services.

Society requires identity systems to enable identity-requiring transactions at scale, putting methods in place that enable the formal asking and answering of identity queries at scale, to allow many day-to-day transactions to occur.

Ineffective identity systems create global challenges for people, for businesses and for society as a whole

Reliance on legacy identity systems that do not effectively enable the transactions that people and entities wish to engage in create challenges for a wide set of stakeholders.

FOR PEOPLE

Service exclusion
Individuals are excluded from key services due to their inability to demonstrate identity

Poor user experience
Services provided to users do not match their needs or are delivered inconveniently

Information overexposure
User information is overexposed, putting users at risk of identity theft and privacy breach

Process inefficiency
Proving identity involves many steps and documents

FOR BUSINESSES

Inefficient service delivery
User-facing processes are cumbersome, resulting in poor customer experience

Obscure risk
Lack of reliable information prevents businesses from accurately calculating the risk of doing business

Fraud
Businesses suffer fraud resulting from stolen or incorrect customer information, or poor authentication

Process inefficiency
Processes provide out-of-date data or require checking multiple sources

FOR SOCIETY

Service exclusion
Entities may be unable to prove attributes and therefore be excluded from key social structures

Service mismatch
Services are delivered incorrectly due to the lack of information

Fraud
Entities can use false information or misrepresent information to gain illicit access to services

Process inefficiency
Processes are highly manual and paper-based, requiring human intervention and remediation

These global identity challenges manifest as specific business problems for FIs

Identity is critical to FIs; their businesses are entirely transaction-based, involving transactions with a high degree of risk and require a high degree of certainty in completion. Global problems with identity therefore manifest as specific business problems for FIs.

ILLUSTRATIVE: BUSINESS PROBLEMS IN FINANCIAL SERVICES

Business problem	Retail / small- to medium-sized enterprise banking	Corporate and investment banking
Inefficient and costly onboarding processes	✓	✓
Inefficient, costly and ineffective know-your-customer (KYC) and due diligence processes	✓	✓
Highly manual and time-consuming compliance processes	✓	✓
Difficulty aggregating information on legal entities and determining total risk exposure	✓	✓
Difficulty attaching individual identity (e.g. corporate directors) to corporate identities	✓	✓
Difficulty identifying all transaction counterparties (e.g. third parties in trading relationships)	✓	✓
Difficulty complying with regulatory standards around data handling and privacy	✓	✓
Multiple views of the customer	✓	✓
Difficulty providing effective/suitable products and services	✓	
Lack of visibility into financial history for new customers	✓	
High fraud rates	✓	
Difficulty tracking asset origination and ownership		✓
Difficulty monitoring and tracking asset rehypothecation		✓

Many of these challenges are driven by the use of physical identity protocols to serve digital transactions

Today's standard identity systems are based on physical documents and processes, which creates many limitations.

CHARACTERISTICS OF PHYSICAL IDENTITY SYSTEMS

Document-based: Identity is based on physical records – the ability to prove identity depends on access and authentication to physical documents (e.g. passports, ID cards and records)

Siloed: Identity information is held in discrete places that are not interconnected and do not enable aggregation, which may be desired by the entity itself or required for some applications

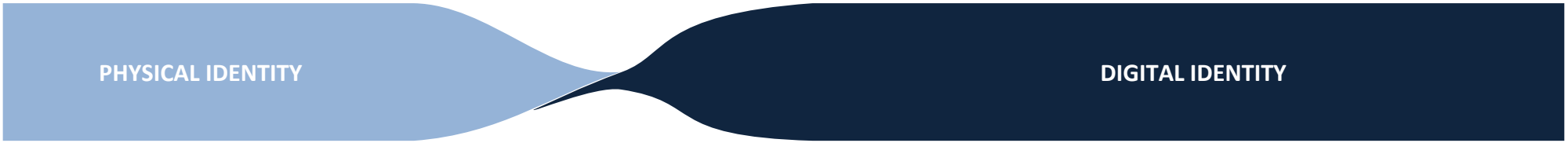
Inflexible: Identity is codified in documents as a limited and standardized set of information about an entity that cannot be easily adapted to transaction requirements

THE PROBLEMS WITH PHYSICAL IDENTITY

- *Proof of identity that is based on possession of physical documents may not require demonstration of a link between an individual and the documents (i.e., authentication), enabling use of an entity's credentials by a different user*
- *Physical identity documents can be falsified, altered or tampered with, as well as lost or stolen*
- *Physical attribute presentation and transfer create the potential for human error in transactions*

THE IDENTITY SHIFT

Identity is now at an inflection point; physical identity systems are breaking down and digital systems are emerging in response.



Physical identity *was designed to enable face-to-face transactions among entities*

The digital economy *is changing the way that identity transactions occur*

Digital identity *enables transactions in the digital world and offers improved functionality for its users*

Digital identity systems support the needs of today's world

Digital identity systems emerged as a direct response to the requirements of transactions in the digital world.

CHARACTERISTICS OF DIGITAL IDENTITY SYSTEMS

Digital-based: Identity exists as a set of digital records that the user can control and use to complete transactions

Interconnected: Proof of identity can be communicated between entities in a standardized, digital format

Flexible: Identity systems adapt to the nature of the transaction, and continuously adapt to requirements by integrating additional information to create a rich view of the user

THE PROMISE OF DIGITAL IDENTITY

- *Digital information can be protected from damage, tampering, loss and theft, with cutting-edge authentication and security protocols*
- *Digital information can be shared in streamlined, tailored and secure ways, predicated on user consent*
- *Institutions can better know and serve their customers, improving existing products and offering new products and services to the underserved*

BENEFITS

Digital identity would deliver a range of benefits to people, businesses and society.

Privacy and control
People would be able to control access to their information

Revenue growth
Financial Institutions would have opportunities to offer Identity-as-a-service

Improved compliance
Regulators would have increased access to trusted, up-to-date information

Improved service delivery
Governments could more easily and effectively deliver public services

New and maturing technologies have important implications for the creation of robust digital identity systems

These technologies may hold considerable promise for identity, and are being explored by many different players.

Data storage

New technologies may offer improved methods of storing user information and increasing user control, privacy and security

- Distributed Ledger Technology combined with encryption and cloud storage allows information to be held and transferred point-to-point in a dispersed, immutable network
- Federated identity standards, such as SAML 2.0, create interoperability between identity management networks and external applications, allowing federated identity systems to scale to large numbers of identity providers and relying parties

Data transfer

Improved attribute exchange protocols allow information to be securely shared between endpoints without risk of interception or decryption, and with more controls that create privacy for users

- Improved encryption protocols, such as Keyless Signature Infrastructure on the blockchain and hashing, provide strong protection for sensitive information and increase the reliability of digital activities
- Data transfer protocols, such as Attributed Based Credentials 4 Trust and zero-knowledge proofs, prevent the creation of metadata by concealing transaction endpoints, increasing user privacy

Authentication

Many new techniques for authenticating users are being explored for their potential to increase information security and user control in certain circumstances by linking users to their digital activities in more robust and persistent ways

- Behavioural and contextual authentication incorporate human and environmental factors to authenticate a user or device
- Biometrics, including fingerprint, retina scanning, heartbeat waveform and facial recognition based on mobile devices have potential to provide greater convenience and security and are being integrated into many anti-fraud controls

Digital identity systems have great potential but also many pitfalls in implementation

Many new identity systems are under development around the world in response to the need for digital identity and new technology capabilities. However, not all have been successful, illustrating some of the pitfalls inherent in the construction of identity systems.

PITFALLS IN IDENTITY SYSTEMS

Stakeholder rejection

- Users may not adopt the system due to poor design or distrust of the system's purpose or structure
- Stakeholders may perceive systems with limited scope and scale as valueless, and therefore not adopt them

Ineffective technology

- A poor technology platform can reduce system functionality, preventing user integration or transaction completion
- Insufficient data protection results in breaches, system compromise and data leakage

Limited support

- Systems that have support from a narrow set of interests may fail due to inconsistent efforts behind their construction and operation
- Systems that lack support from all key stakeholders may not experience sustainable and continuous uptake

Unsustainable operation

- Systems with unsustainable operating or business models will fail

Policy Changes

- Large, complex and emotive programmes such as ID cards can be susceptible to political and / or ideological shifts

Examples of identity system challenges are common…

Hack Brief: Turkey Breach Spills Info on More Than Half Its Citizens
- WIRED, April 2016

Philippine electoral records breached in 'largest ever' government hack
-The Guardian, April 2016

Aadhaar Bill passed in Lok Sabha, Opposition fears 'surveillance'
-Indian Express, March 2016

South Korea at a crossroads with ID card, data theft losses
-CBC News, October 2014

The National [UK] Identity Card scheme will be abolished within 100 days with all cards becoming invalid
-BBC News, May 2010

Identity Primer

Identity is the frontier of privacy and security in the digital world

In an increasingly borderless and digital world, privacy and security cannot be ensured through the construction of walls around sensitive information

Identity is the new frontier of privacy and security, where the very nature of entities is what allows them to complete some transactions but be denied from completing others

To understand the importance of identity and the criticality of strong identity protocols that protect against cyber-risk and suit the needs of transacting parties, it is essential to understand what identity is, and its role in enabling transactions

9-Figure Deals Lift Cybersecurity Investments To An All-Time High
-Forbes, February 2016

Cybersecurity top on government agenda
-Times of India, February 2016

In Today's Era of Data Breaches, Are You Sure Your Data Is Protected?
-Security Intelligence, January 2016

1 in 3 Americans Victim of Healthcare Data Breach in 2015
-Information Management, February 2016

U.S. presses retail banks to help millions of 'unbanked' Americans
-Reuters, February 2016

How to Fight Tax Identity Theft
-Huffington Post, February 2016

FCA fines Barclays £72 Million for poor handling of financial crime risks
-Automated Trader, November 2015

Identity is a collection of pieces of information that describe an entity

Identity is not a monolith; it is a collection of individual attributes that describe an entity and determine the transactions in which that entity can participate. While the total existing set of attributes is endless, they can be broadly categorized into three groups: inherent, inherited and assigned attributes. These attributes differ for members of three main user groups: individuals, legal entities and assets.

	For individuals:	For legal entities:	For assets:
INHERENT ATTRIBUTES Attributes that are intrinsic to an entity and are not defined by relationships to external entities.	• *Age* • *Height* • *Date of birth* • *Fingerprints*	• *Industry* • *Business status*	• *Nature of the asset* • *Asset issuer*
ACCUMULATED ATTRIBUTES Attributes that are gathered or developed over time. These attributes may change multiple times or evolve throughout an entity's lifespan.	• *Health records* • *Preferences and behaviours (e.g. telephone metadata)*	• *Business record* • *Legal record*	• *Ownership history* • *Transaction history*
ASSIGNED ATTRIBUTES Attributes that are attached to the entity, but are not related to its intrinsic nature. These attributes can change and generally are reflective of relationships that the entity holds with other bodies.	• *National identifier number* • *Telephone number* • *Email address*	• *Identifying numbers* • *Legal jurisdiction* • *Directors*	• *Identifying numbers* • *Custodianship*

Specific attributes enable entities to complete certain transactions

Identity is the total set of an entity's attributes. These attributes enable entities to participate in transactions, by proving to their counterparty that they have the specific attributes required for that transaction.

EXAMPLE: Users and transactions

Individuals	Legal entities	Assets
To purchase alcohol, users must prove that they are over the legal drinking age in that jurisdiction	*To onboard with a FI, the entity must have proof that it is a legal and non-sanctioned entity*	*Asset trading, such as trading of equities on a stock exchange, requires proof of ownership and origination*
To vote, users must prove that they are over the legal voting age, have citizenship and reside in that jurisdiction	*To transact in capital markets, the entity must have proof that it is a legal and non-sanctioned entity with an acceptable risk profile*	*Transfer of title of an asset requires proof of ownership from the entity that is transferring the asset*
To open a bank account, users must prove that they are a non-sanctioned person who is legally allowed to engage in financial transactions		

Note: Assets have identity, but are unable to act or transact on their own. Assets require custodians who are entitled to act or transact on the asset's behalf.

Identity transactions have three main aspects

Authorization	*Attributes*	*Authentication*
What must be true about the users to complete the desired transaction?	*Can users prove that they are eligible to complete this transaction?*	*Do the attributes being presented genuinely belong to the entity that is presenting them?*
Authorization is a function of the transaction and the transaction counterparty; they will determine the requirements for transaction eligibility, and make a query about certain user attributes (e.g. age, address).	Users must present their proof of attributes in response to the query. Once users present the required attributes, the counterparty must determine if they are reliable.	The counterparty will determine whether the attributes match the presenting users. If the users are able to authenticate the attributes, the transaction can proceed.

Repeated identity transactions

This model of identity transaction applies to onboarding transactions, that is, transactions where the counterparties do not have an established relationship or where the counterparty is required to gather identity information with every transaction.

Some identity relationships may have a single onboarding transaction; after initially onboarding the users and verifying them through a full identity transaction, the counterparty may use an authentication method (e.g. username and password, chip-and-PIN card) for each subsequent transaction. This allows them to verify that the same entity is transacting each time without going through the full identity transaction process.

*Note: Not all transactions require **exact knowledge** of attributes. Many transactions simply require attribute data to fall inside certain parameters (e.g. instead of knowing an individual's birthdate, a transaction may only require that the user be over a certain age); this is critical in constructing privacy-enhancing identity systems.*

Different identity transactions require different levels of assurance

The level of assurance (LoA) in an identity transaction is the degree of certainty that the transacting parties have in the veracity of the identity being presented.

ASSURANCE IN TRANSACTIONS

A high LoA in identity transactions is not always desirable, as a high LoA requires intensive onboarding and strong authentication processes that may be cumbersome for the user. The LoA required in an identity transaction should therefore generally be dependent on risk – the risk level of the transaction and the consequences of error.

DETERMING ASSURANCE LEVELS

The level of assurance of a given transaction is determined by two main factors:

1. Registration protocols: How stringently the identity provider verifies attributes when onboarding users
2. Authentication method: The strength of the authentication method used to complete transactions between the identity provider and the relying party

Low assurance transactions

Transactions that do not involve a release of information and only involve an information flow from the user to the relying party are low-assurance transactions

Examples include online registrations (e.g. signing up for a news site) and some payments (e.g. paying a parking ticket online)

High assurance transactions

Transactions that involve the release of sensitive and private information, or the transfer of money or assets, are high-assurance transactions

Examples include banking and other financial transactions, such as using an online brokerage account, and many government services

Identity systems tend to evolve inside natural boundaries…

Identity exists within networks that enable transactions between the entities inside that network. These networks tend to evolve around user groups with similar needs and characteristics. These boundaries form what are called “natural identity networks”. Every natural identity network has different needs and therefore will require different system configurations.

NATURAL IDENTITY NETWORKS

The networks that form inside the natural boundaries of identity systems for individuals are based on **geographic location** or **affiliations with a supervisory entity**

Examples include national identity systems, state or provincial identity systems, and employee management systems

The networks that form inside the natural boundaries of identity systems for legal entities are based on **national affiliation, industry** or **geographic reach**

Examples include national or global business registries and industry identifier systems

The networks that form inside the natural boundaries of identity systems for assets are based on their **asset class, origination** or **ownership**

Examples include registries of assets of a single class, or registries of assets that are all owned by a single entity

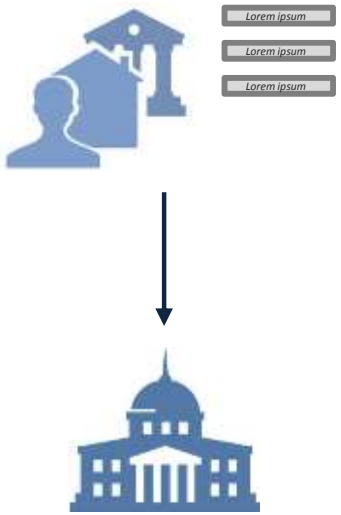
… and operate on a basic shared structure

The purpose of a formal identity system is to allow counterparties without a previously established relationship to engage in trusted transactions.

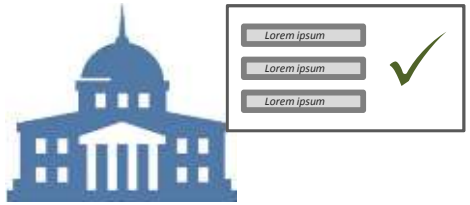
- In a formal identity system, the users' attributes are attested to by trusted third parties; these third parties issue credentials that tie their attestation to the specific attributes, with some method of authenticating the credential to the entity that is presenting it
- Users can use their wallet of credentials to engage in transactions with other entities that require some proof or knowledge of their attributes

THE STRUCTURE OF IDENTITY SYSTEMS

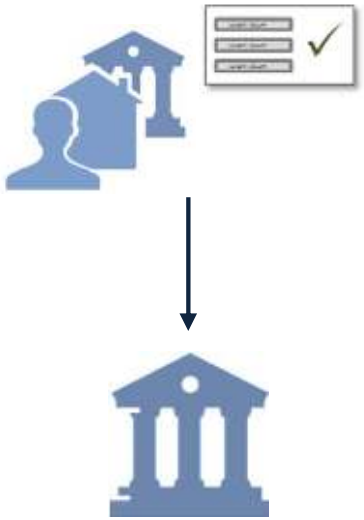
1. *The user presents a set of attributes to a third party*



2. *The third party verifies the attributes and attaches its attestation to the attributes, becoming an identity provider for the user*



3. *The user then uses the credential from the identity provider in transactions with relying parties*



Certain roles and functions must exist in every identity system

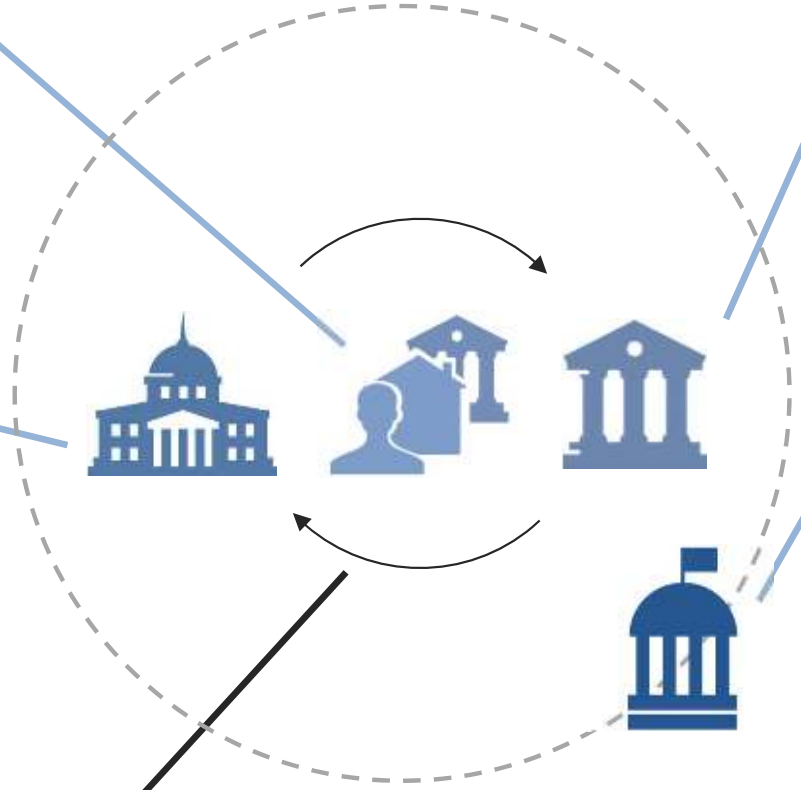
Every identity system must have four roles and one function to operate.

Users

Users are entities for which the system provides identity, for the purpose of allowing them to engage in transactions

Relying parties

Relying parties (RPs) are entities that accept attestations from identity providers about user identity to allow users to access their services



Identity providers

Identity providers (IdPs) are entities that hold user attributes, attest to their veracity and complete identity transactions on behalf of users

Governance body

The governance body provides oversight for the system and owns the operating standards and requirements

Attribute exchange platform

The attribute exchange platform completes transactions by matching identity queries from RPs with attributes from IdPs and exchanging attributes or proof of identity

Role
Function

Methods have evolved, but the concept of identity proofing has not changed over time

The fundamental concept, purpose and structure of identity systems have not changed over time, while methods and technology have made huge strides forward.

Past → **Present**

A letter of introduction is one of the oldest forms of identity documentation.

- **User:** Individuals would use a letter of introduction as an attestation of identity and character to someone they did not know
- **IdP:** The letter writers would provide attestations for various attributes of the users (e.g. that the user was a person of good character)
- **RP:** The recipients of the letter would choose whether or not to accept the attestations based on their knowledge of the IdP and their evaluation of the letter's veracity

Today a passport issued by an individual's country of residence or origin is one of the most common, trusted identity documents.

- **User:** Individuals are often asked to present their passport to complete transactions that require proof of identity (e.g. entering new countries, opening a bank account, etc.)
- **IdP:** The government of that country acts as an IdP, making certain attestations about the user
- **RP:** The attestations made by the IdP are accepted by a RP based on its trust in the document, its issuer and its evaluation of whether the bearer is the true owner of the passport

Digital identity allows identity transactions to be completed through digital channels

A digital identity system has the same basic structure as a physical identity system, but attribute storage and exchange are entirely digital, removing reliance on physical documents and manual processes.

FEATURES OF DIGITAL IDENTITY SYSTEMS

Digital information storage and transfer

- User identity information is captured and stored in digital form
- User identity information is transferred between IdPs and RPs in digital form
- Form factors, such as computer or mobile devices rather than physical documents, can be used to complete transactions

Direct connectivity

- Information transfer occurs directly between IdPs and RPs, without an intermediary (although user consent can be built in) and without manual intervention (e.g. physical information entry)

THE CURRENT LANDSCAPE OF DIGITAL IDENTITY

Digital identity is not a new concept; many identity systems exist in the world today that either incorporate some digital elements or are entirely digital-based systems. The landscape of digital identity solutions is explored further in the next section of this report. These systems exist along a spectrum of maturity and degree of sophistication; however, all are designed to capture some of the benefits that digital identity brings over traditional physical-based identity systems.

Digital identity offers significant benefits over physical identity systems

Beyond offering new functionality, digital identity has significant functional benefits over physical-based identity systems.

Security

- ✗ Physical identity documents can easily be lost, stolen or replicated by illicit actors, as well as read by entities with no legitimate reason to have the user information
- ✓ Digital identity information could be stored, transferred and exposed using cutting-edge digital security protocols that would prevent against data breach, modification, loss and theft

Privacy and control

- ✗ Physical identity does not allow the release of information to be tailored to the identity transaction; identity documents display a fixed set of information that can be read by almost any entity
- ✓ Digital identity allows individuals to control the sharing of their information, to expose the minimum amount of information required for a given transaction, and shield their information from illicit access

User experience

- ✗ Physical identity requires users to manually show documents or enter identity information in transactions, resulting in a cumbersome user experience and creating potential for human error in transactions
- ✓ Digital information transfer would streamline the transaction process for users and RPs across all channels, increasing the ease of transacting for both parties and removing the potential for human error

Flexibility

- ✗ Physical identity results in the crystallization of user identity in physical documents, and a fixed view of identity that cannot be expanded to cover additional user attributes
- ✓ Digital identity would provide a flexible and scalable system that could incorporate a greater richness of identity information than is currently possible

The Landscape of Digital Identity Systems

Many digital identity systems exist in the world today, serving various natural networks

The digital identity systems that exist today fall across broad ranges of purpose, scope and sophistication. Some systems have a digital element bolted onto what is still fundamentally a physical identity system, while others are fully digital and are built to scale and expand as user needs evolve.

Disparate identity systems were studied, including systems for all user groups, to understand the landscape of digital identity solutions, categorize these systems and draw high-level conclusions on which systems best suit different needs.

TYPES OF DIGITAL IDENTITY SYSTEMS

Systems for individuals

The majority of identity systems are designed for individuals, and are often government-driven systems

Purpose:

Designed to increase financial or social inclusion and streamline the delivery of services, or to control access to internal systems for a single organization

Systems for legal entities

Identity systems for legal entities often take the form of centralized registries of information that are owned by a single government or utility

Purpose:

Intended to standardize data across entities, streamline processes and enable data aggregation at a macro level

Systems for assets

Identity systems for assets often take the form of a centralized registry or an internal system for a single organization

Purpose:

Intended to clarify ownership, standardize data or enable the operation of networked systems

The most significant differences in identity systems fall across three primary dimensions

Primary dimensions of choice are the set of choices that must be made in the design of a digital identity system that have the greatest impact on the system's function and structure.

These are not always conscious choices; they are often a natural outcome of the setting in which the system is being implemented, and the problem that the system is intended to solve or the needs that it is intended to serve. The three primary dimensions of choice are:

Nature of identity provision

Is there a single source of identity information? Are there a limited set of parties who provide attributes? Is identity provision distributed across many different entities?

Centralized: One entity stores and provides the identity information

Federated: A limited number of entities store and provide identity information

Distributed: Many different entities store and provide identity information

Number of relying parties

Is there a single RP that can access user attributes, or are there many RPs that can access user information?

One: The system has a single RP that is able to access identity information

Many: The system incorporates many RPs that are able to access identity information

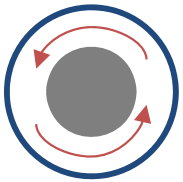
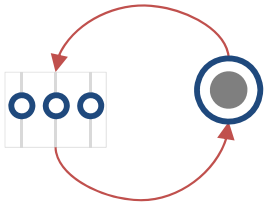
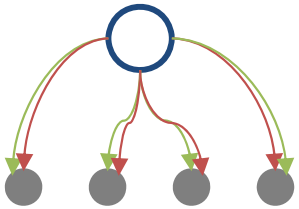
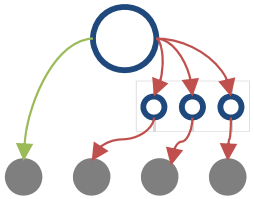
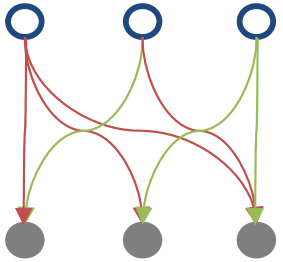
Nature of information transfer

Is information transferred from the IdP to the RP for the purpose of authenticating a user, or is there a transfer of user attributes that the RP requires to execute a given transaction?

Authentication: The IdP authenticates the user for the RP, allowing the RP to complete transactions using information or records that the RP holds

Transaction: The RP requires information from the IdP for the purposes of completing a transaction for the user

We have defined five distinct archetypes that exhibit significant differences in structure and purpose

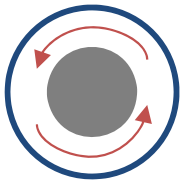
	Internal identity management	External authentication	Centralized identity	Federated authentication	Distributed identity
Structure	 One entity acts as both the IdP and RP	 Many IdPs authenticate users to a single RP	 One IdP serves many RPs	 A set number of IdPs authenticate users to many RPs	 Many IdPs serve many different RPs
Flow of information	• The system provides users within a single network access to services that they are permissioned to access based on their attributes • All user attributes are held inside the single entity and are used to permission users to either grant or deny access to a given service or pathway	• The system authenticates users to the RP based on their authentication to one of a set of IdPs • No attributes are transferred between the IdPs and the RP; the authentication transaction is used to simply grant or deny the user access to the services offered by the RP	• The system has a single IdP that authenticates users and transfers or exposes attributes to many different RPs	• The system has a single IdP that stores user information, while a separate set of IdPs authenticate users who are attempting to transact with RPs • After authentication, the requested attributes are transferred from the IdP that holds attributes to the RP with which the user is transacting	• The system involves multiple IdPs that authenticate users and transfer attributes to many different RPs

Identity provider (IdP) — *Attribute flow*

Relying party (RP) — *Authentication flow*

Internal identity management solutions are designed for use by one entity

INTERNAL IDENTITY MANAGEMENT



In internal identity management systems, the same entity acts as an IdP and a RP. The entity uses information that it holds on users to permission them to access various internal services.

A good example of an internal identity management system would be a company or a government that permissions its employees or citizens to access different services based on their attributes.

KEY ARCHETYPE FEATURES

- The IdP/RP owns the required attributes needed to determine user permissions within the organization
- The system is used to control which users within a single organization or entity have permission to access certain services
- These types of solutions are generally developed by private organizations and sold as a product or service to various entities and institutions

CASE STUDIES

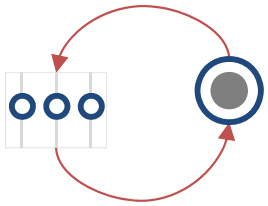
Closed Internal Management Systems

Private solutions, global

Leading software as a solution (SaaS) providers such as Salesforce, Oracle, SAP and Microsoft provide solutions that help their customers better understand, manage and interact with a set of users. SaaS has become a common delivery model for many business, as these solutions help keep users, data and applications within a closed system secure. These solutions serve a variety of industries and user groups (e.g. customers, employees, citizens, etc.).

External authentication systems facilitate access to high-traffic services

EXTERNAL AUTHENTICATION



In external authentication systems, one entity acts as both the IdP and the RP but uses an additional external set of IdPs to authenticate its users. The purpose of this system is to improve user experience for individuals or businesses when accessing online services; these users can use existing logins rather than maintaining multiple usernames and passwords for each service.

KEY ARCHETYPE FEATURES

- The system has one RP, often a government, that holds user information and leverages a set of established institutions as IdPs (e.g. FIs, telecom providers)
- The IdPs are usually trusted entities that perform strong authentication in user onboarding and are therefore trusted to provide a high level of assurance in identity transactions
- Users can use their existing authentication methods through this group of IdPs to gain access to the RP's services
- Both the RP and IdPs store user attributes – the authentication system is used to verify that the entity authenticating through the IdP should be permitted to transact with the RP
- No attributes are transferred from IdPs to the RP

CASE STUDIES

GOV.UK Verify

Public-private programme, United Kingdom

The GOV.UK Verify programme is an external authentication system that allows UK citizens to access government services online. Users verify their identity online with one of nine IdPs. Once the users are authenticated through one of these providers, they are granted access to the government service they are trying to access.

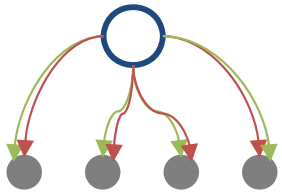
SecureKey Concierge

Public-private solution, Canada

SecureKey Concierge is a digital authentication system that allows individuals to choose a trusted credential they already have with one of a set of FIs to access government services online. The users log in with their online banking username and password and are authenticated by their bank. Once authenticated, the users are granted access to the service. No attributes are transferred in the system.

Centralized identity systems use one IdP as a single source of truth

CENTRALIZED IDENTITY



In centralized identity systems, a single entity acts as an IdP that authenticates users to RPs and transfers their attributes. These systems are often designed to streamline service delivery, enable data aggregation and provide a single view of users across multiple RPs.

KEY ARCHETYPE FEATURES

- A single IdP holds all user attributes and owns the identity system; this is often the government or another central governing body
- The IdP authenticates the user to the RP and transfers either a fixed or a tailored set of attributes to the RP to enable it to complete a transaction on behalf of the user
- Some systems require RPs to pay a fee to use the system and to gain access to user attributes
- Identity information can be transferred directly through a physical form factor (e.g. a smart card) or through a digital brokerage system

CASE STUDIES

DigID

Government programme, Netherlands

DigID is a digital authentication system for Dutch residents who are accessing government services online. Individual attributes are held in a national citizen registry; these attributes are used to authenticate users when they apply for a DigID. Individuals can then use their DigID username and password to authenticate themselves to government agencies. Their national identifier number is transferred from the national citizen registry to the RP.

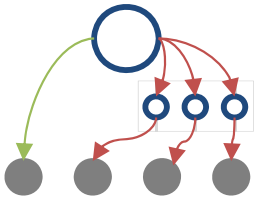
Population Registry

Government programme, Finland

The Population Registry is a national database that is owned and maintained by the Finnish government. The government acts as the IdP, transferring attributes to public and private RPs. The purpose of the system is to collect data that can be used for elections, tax filing, judicial administration, etc. Private RPs may also access this data if they pay a fee and have received user consent.

Federated authentication systems rely on third parties to grant user access to services

FEDERATED AUTHENTICATION



In federated authentication systems, one IdP uses a set of third parties to authenticate users to a range of RPs. The primary IdP is the entity that stores and transfers user attributes. These systems are designed to improve the login and transaction processes for users who are accessing online services by allowing them to use a single set of credentials to authenticate, and transferring attributes to RPs on their behalf.

KEY ARCHETYPE FEATURES

- Identity information is stored centrally by one IdP
- A set of third-party IdPs act as brokers that authenticate users to the RPs with which they are attempting to transact
- RPs are able to access user attributes from the primary IdP, often for a fee; many systems also require explicit user consent for attributes to be transferred
- In systems that allow for the discretionary transfer of attributes rather than a fixed set of attributes, the user must explicitly consent to the transfer of specified attributes from the primary IdP to the RP
- These systems are often government-driven, and the government acts as the central IdP that holds citizen or entity data

CASE STUDIES

NemID

Private sector solution, Denmark

NemID is an electronic ID, digital signature and secure email solution that provides individuals access to public and private services. The government tendered the system to the private sector. Users use a common NemID login and password, as well as unique one-time passwords to authenticate themselves to online services. User attributes are stored in a central registry.

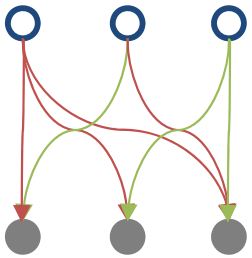
Sweden BankID

Public-private service, Sweden

Sweden has established an eID system that provides citizens and businesses access to over 300 public and private services. Digital identities are issued by a set of private entities, including large banks and a major telecommunications provider. The public sector buys identity validation services from the private sector. Private sector service providers can join the BankID system by signing contracts with eID providers for authentication. The solution has been very successful; over 9 million citizens currently use the service.

Distributed identity systems connect many IdPs and RPs

DISTRIBUTED IDENTITY



In distributed identity systems, many IdPs collect, store and transfer user attributes to many RPs. These systems are notable in that they do not rely on attributes from a single IdP. The purpose of these systems is to allow users to interact easily with many different entities in an online environment by giving them a digital "wallet" of credentials.

KEY ARCHETYPE FEATURES

- Identity information may be stored by multiple IdPs, on a distributed protocol (e.g. blockchain), or may be collected from a variety of sources and aggregated by a single entity that operates the system
- Attributes can be transferred from IdPs to RPs through a variety of methods, including smart cards or digital/mobile protocols
- These systems are often privately owned and funded; governments or other public sector bodies may not play an active role within the network
- Users own their own identities and often control which transactions occur and what attributes are transferred from one or more IdPs to the RP
- These systems may not have a governance body and instead rely on common operating standards for interoperability

CASE STUDIES

TUPAS

Private sector solution, Finland

TUPAS is an identity system in which over 10 banks act as IdPs. Individuals can log into a wide range of services with credentials from their bank. The users' full names and National ID numbers are transferred from the IdP to the RP.

Global Legal Entity Identifier Foundation (GLEIF)

Non-profit organization, global

GLEIF supports the implementation of the Legal Entity Identifier (LEI) standard. This system assigns LEIs to every entity that engages with FIs; entities can use their counterparty's LEI to access their identity information from the GLEIF's partner network.

Mobile Connect

GSMA, global

Mobile Connect is a digital identity system that authenticates the users through their device, allowing users to access a variety of services. This eliminates the need for users to have many usernames and passwords to access online services.

The potential of blockchain technology in identity

Blockchain, or distributed ledger technology (DLT), is a technology protocol that allows data to be shared directly between entities in a network, without intermediaries. DLT has certain key features that hold potential for identity systems:

FEATURES OF DISTRIBUTED LEDGER TECHNOLOGY

Low transaction cost

Distributed ledgers eliminate the need for intermediaries and therefore lower the cost of completing transactions

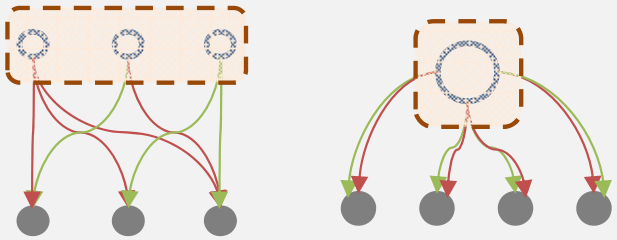
Immutability

Transaction history is maintained and verified through the network, preventing the falsification of information

Convenience

Record-keeping and transactions can be executed from any device, on- or offline

Illustrative: Applications of DLT in digital identity



DLT has potential in identity applications as an information storage and transfer mechanism within different archetypes. DLT could be applied as a distributed protocol, giving users the ability to store their identity attestations on a ledger and expose them to different RPs, or in a centralized system where the ledger would be owned by a single entity that would provide a consolidated view of the users' attestations for use in transactions, but would not reveal the nature of the credentials.

Many initiatives are currently underway that explore the true potential for DLT in identity systems; this report will not explore this topic in detail.

The Right Solution for the Right Problem

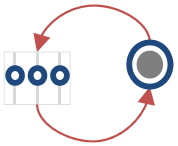
The archetypes of digital identity are built to serve very different needs

Internal identity management

Best suited to: manage user permissions inside a single entity based on internal information, to ensure the right individuals have access to the right resources and endpoints

Example: Large organizations that need an identity access and management solution to control access to their internal services with a select user group (e.g., employees, customers, etc.)

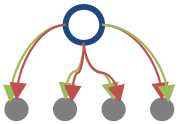
External authentication



Best suited to: streamline user access to a suite of services that are offered by a single entity and eliminate proprietary logins

Example: A government offering its citizens online services that are critical but infrequently used

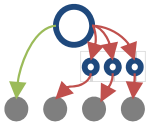
Centralized identity



Best suited to: provide a single version of the truth and a complete, accurate and standardized view of non-confidential data across different users

Example: An industry utility offering a comprehensive view of the entities in that industry to manage risk and exposure

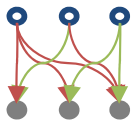
Federated authentication



Best suited to: provide a single version of the truth and a complete, accurate and standardized view of data while allowing users to authenticate to a set of third parties, thereby eliminating proprietary logins

Example: A government enabling identity transactions for its citizens through collaboration with third parties

Distributed identity



Best suited to: incorporate large numbers of IdPs and RPs, providing user convenience, control and privacy in an online environment

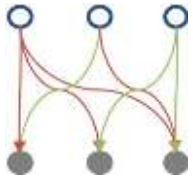
Example: A full digital economy requiring multiple independent connections between IdPs and RPs to enable user transactions

Two of these archetypes are well suited to solve broad identity problems

Centralized and distributed identity systems are best suited to provide digital identity at scale; however, these two archetypes are not equally well suited to provide identity for different user groups.

FOR INDIVIDUALS

Distributed identity

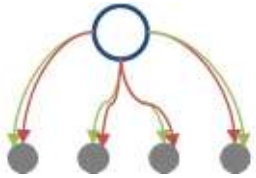


Distributed identity systems are the best fit to provide identity for **individuals** at large scale

- Distributed identity systems are built to scale to large numbers of IdPs and RPs, enabling a full set of convenient and efficient transactions for users
- These systems protect user privacy and increase control by allowing users to choose which entities hold their information, and by removing a single point of failure from the system

FOR LEGAL ENTITIES AND ASSETS

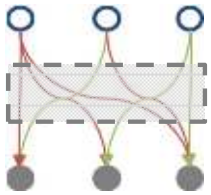
Centralized identity



Centralized identity systems are suitable to provide identity for **legal entities** and **assets** on a large scale

- Centralized identity systems offer a consolidated and standardized view of identity information, and offer the single source of truth that is required for transactions involving legal entities and assets to deliver key value to external stakeholders such as regulators

Distributed identity



Distributed identity systems are also suited to provide identity for **legal entities** and **assets** on a large scale; however, these identity systems should have a "wallet" or aggregation layer that can provide a consolidated view of the user

- Distributed identity solutions offer identity at scale, and an aggregation layer provides the single view of the user required for legal entities and assets

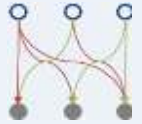
The centralized and distributed identity archetypes would also solve many of the business challenges that FIs are currently experiencing

IN RETAIL / SMALL- TO MEDIUM-SIZED ENTERPRISE BANKING

The need:

- Trusted, up-to-date individual identity information
- Ability to access additional user attributes with consent
- Ability to internally link identity information to provide a single view of the customer
- Secure repositories for user information to prevent identity theft due to stolen data

Distributed identity



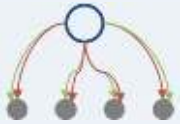
Distributed identity for individuals would allow FIs to access trusted user information and link it back to a single user identity; it would also ensure that user information would be securely stored with redundancy in the case of breach.

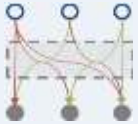
IN CORPORATE AND INVESTMENT BANKING

The need:

- Trusted, up-to-date user identity information
- Visibility into asset and user identity information
- Ability to link asset, entity identity and individual information
- Ability to aggregate identity information across entities

Centralized identity | **Distributed identity**



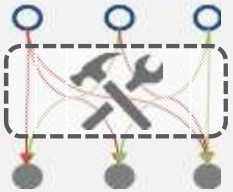


Centralized identity and **distributed identity with an aggregation layer** for legal entities and assets would allow FIs to have a consolidated, trusted source of digital attributes for these users.

Configuring and implementing an identity system require many additional choices beyond archetype selection

Configuring an identity system requires choices to be made against a secondary set of dimensions that do not have the key functional and structural importance of the primary dimensions, but have strong impact on how the system will operate. The choices made against the secondary dimensions should therefore be tailored to suit the specific needs and requirements of the natural identity network.

ILLUSTRATIVE: SECONDARY DIMENSIONS OF CHOICE



Types of IdPs and RPs: What types of entities are allowed to act as IdPs and RPs in the identity system?

Broker mechanism: How are RP queries connected with IdP attestations? Can the system support attribute exposure and attribute inquiry transactions? Does the system support transaction blinding?

Data management: Where are data stored - in a central database, on a smart card, on a distributed protocol (e.g. blockchain)? Are user attributes aggregated by a third party?

Scaling: Is the system designed to scale beyond its initial set of applications?

Business model: What is the business model that supports the system? Who funds the system?

Governance: Who is responsible for system governance and oversight? Who is responsible for system operation?

User rights: What level of control do users have over the information that is held on the system, who holds it, and when and how it is shared?

Note: This is not an exhaustive list of choices; many further choices must be made

It is impossible to provide an exhaustive list of the secondary dimensions of choice in the configuration and implementation of an identity system, or to give recommendations against each. A set of guiding principles has therefore been developed to steer secondary decision-making and to assist in delivering a robust identity system that suits the needs of its stakeholders.

Guiding Principles

The guiding principles shape the choices that need to be made against the secondary set of dimensions

A successful natural identity network is a product of the choices made against the secondary dimensions. Five principles inform decision-making around these choices and guide the development of robust, value-accretive systems.

GUIDING PRINCIPLES FOR DIGITAL IDENTITY

Social good

The system is designed as a social good that is available to all users and will deliver maximum benefit to a range of stakeholders

Privacy-enhancing

User information is only exposed to the right entities under the right circumstances

User-centric

Users have control over their information and can determine who holds and accesses it

Viable and sustainable

The system is sustainable as a business and is resilient to shifting political priorities

Open and flexible

The system is built on open standards to allow scaling and development; standards and guidelines are transparent to stakeholders

Identity systems should provide identity to all users, serve user interests and be accessible to all entities that wish to transact within them

SOCIAL GOOD

BACKGROUND

The ability to prove identity allows users to be integrated into formal financial and social systems and engage in necessary and basic day-to-day transactions; digital identity should therefore be considered a social good to which all entities should have access.

IMPLICATIONS

- The system should be designed to scale to all users and network stakeholders who wish to participate
- The public sector should have some involvement in defining the system's operating parameters and regulatory standards to ensure user interests are protected and to increase the scale of the system
- System access mechanisms (e.g. mobile platforms) should democratize access

IMPLICATIONS FOR FIs

- FIs have relationships with a large numbers of users; this scale can act as a catalyst in driving system adoption and uptake
- FIs have a key role to play in ensuring that identity systems are a tool to increase financial inclusion

CASE STUDIES

SASSA

Public-private partnership, South Africa

The South African Social Security Agency, Grindrod Bank and MasterCard have issued biometric enabled debit cards to over 22 million social security recipients. The SASSA card holds an individual's personal information on the chip, is authenticated through biometrics (fingerprint and voice pattern) or a personal identification number (PIN), and is linked directly to a bank account where social grants are deposited.

The end result is over 5 million people becoming financially included, and huge efficiencies in the distribution of social grants in South Africa.

Identity systems should be privacy-enhancing, protecting user information from illegitimate access, accidental exposure and overexposure

PRIVACY-ENHANCING

BACKGROUND

Current identity systems put users at risk, leaving user information vulnerable to privacy infringement, data leakage and overexposure. A digital identity system should protect user information, ensuring that only what is needed is revealed to RPs, and that these parties are only using the data for the disclosed purposes.

IMPLICATIONS

- All attributes, including demonstrated behaviour and preferences, should be covered in an identity system
- Attribute transfer should use new information exchange protocols that allow endpoint blinding
- The brokerage mechanism that connects the endpoints of identity queries should allow only the minimum required information to complete attribute inquiry or attribute exposure transactions to be exposed to the RP
- Attributes should only be stored by IdPs with adequate data security (as defined by system standards)
- Users or custodians should have visibility into requested identity transactions and a defined recourse method if their information is being misused
- The storage of sensitive information should be non-centralized to reduce the severity of consequences and the impact on users in the event of a data breach

IMPLICATIONS FOR FIs

- FIs should build cyber-resilient identity systems and meet standards set by the governance body around data protection and storage
- FIs will need to seek user consent to gain access to or share attributes

CASE STUDIES

TUPAS

Private identity solution, Finland

In the Finnish TUPAS system, a set of FIs act as IdPs and transfer user information on their behalf to RPs. The user has visibility into which attributes are being requested by the RP, and must provide consent for the exchange to occur .

Drivers' Licences

Government solutions, global

Traditional drivers' licences are a commonly used form of identity. However, they compromise privacy by permitting the RP to read all the user's information, rather than just the information required for the transaction.

Identity systems should give users control over the storage and transfer of their personal information

USER-CENTRIC

BACKGROUND

Many identity systems have failed due to a lack of user uptake, driven by concerns around the function and purposes of these systems. A successful digital identity system that serves as a social good should place the user (or the user's custodians) in control over identity information.

IMPLICATIONS

- The mutuality of identity should be considered; users or custodians must have clear visibility into who is requesting their information and for what purpose
- Identity transactions should require consent; exceptions must be clearly defined and communicated, and users should be advised of when their information has been accessed
- Users should be able to revoke consent
- Users should have control over where their personal information is stored
- Users should be able to easily update their information with IdPs

IMPLICATIONS FOR FIs

- FIs will be able to request identity information from users in order to tailor products and services
- FIs will require user consent to share identity information

CASE STUDIES

ConsenSys

Private solution, USA

In the ConsenSys system, users are able to upload their information and have complete control over who their data are exposed to. Users do not choose who stores their data because all identity information is stored on uPort – a user-controlled application that operates on the blockchain.

SecureKey Concierge

Public-private solution, Canada

The SecureKey Concierge system allows Canadian citizens to access government services online by authenticating through any of a large number of FIs with which they already transact.

Identity systems should be designed as businesses that are viable and sustainable in the long term

VIABLE AND SUSTAINABLE

BACKGROUND

Implementing a digital identity system represents a significant effort for all stakeholders; stakeholders must have assurance that their investment will be worthwhile. The system must therefore be designed as a viable and sustainable project.

IMPLICATIONS

- The public sector should have some role in system development and implementation to represent user interest, to drive uptake and to ensure regulatory participation
- The private sector should be involved in system development and implementation to provide executional ability, and operational viability and ensure the system is cost-effective
- Both the public and private sectors should play a role in developing operational standards, including:
  - Liability and dispute resolution
  - Business model
  - Information collection, storage and transfer
  - Levels of assurance
  - Technical requirements
  - User consent models
  - Auditing

IMPLICATIONS FOR FIs

- FIs have a key role to play as important and trusted private entities in shaping the system's operational requirements and standards
- FIs will have the opportunity to monetize identity-as-a-service

CASE STUDIES

National ID Cards

Government solution, United Kingdom

The UK government introduced national ID cards as a personal identification document. The system was scrapped in January 2010, as the incoming government stated the system was "wasteful, bureaucratic and intrusive", posing a significant threat to the privacy and security of personal information.

Clarient Entity Hub, DTCC

Private identity solution, global

Clarient Entity Hub is a utility designed to manage data and regulatory complexity for parties engaging in financial transactions. It aims to increase transparency across financial markets and is offered as a paid service to other entities.

Identity systems should be built on open technology and data standards, and should be designed to integrate new parties and serve changing user needs

OPEN AND FLEXIBLE

BACKGROUND

Identity systems that are static and designed for a single purpose are by nature limited in scope and have low resilience to environmental changes. A resilient identity system should accommodate changing requirements and integrate new parties.

IMPLICATIONS

- The system must be built on open technology standards
- The system must be built on open data standards
- The system must have clear standards around IdPs and RPs, such that new entities can join the system and adhere to all standards and requirements
- The system must have a governance body that will continuously adapt requirements and standards and monitor system performance

IMPLICATIONS FOR FIs

- Open technology and data standards will reduce barriers to users switching institutions

CASE STUDIES

X-Road

Government solution, Estonia

The Estonian digital identity system is built on a common technology framework, called X-Road. This framework creates interoperability between different databases, hugely increasing the digital identity system's functionality and effectiveness.

European Union E-Identity Legislation

Public sector solution, EU-wide

The EU E-Identity legislation sets requirements for member states issuing identity to citizens to ensure mutual recognition and scale of identity systems across Europe.

The established implications should help guide decision-making around configuring identity systems

Building a successful identity network is difficult. A series of choices need to be made to ensure the system delivers value to all stakeholders and gains traction and acceptance.

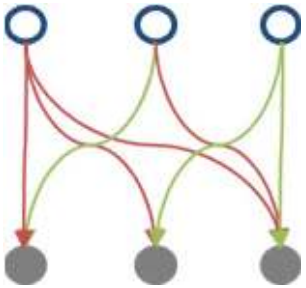
- The highest-level considerations in the development of an identity system are the user group and the need that the system will serve, and the archetype structure that should therefore be considered.
- Once these considerations have been settled, the secondary dimensions of choice should be considered against the guiding principles of digital identity.

1
Problems and user groups

The highest consideration is the user group and the problem that the identity system is designed to solve; this will determine the limits of the natural identity network

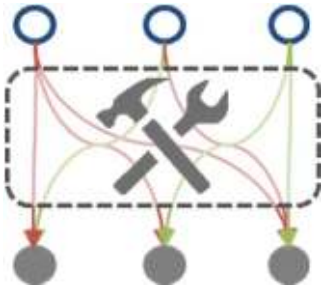
2
Primary dimensions of choice

The user group and target problem will guide the selection of an appropriate identity archetype



3
Secondary dimensions of choice

The guiding principles for identity and their implications will help determine what structural and configuration choices should be made against the secondary dimensions of choice



These implications are meaningful for entities within the digital identity network

When configuring identity systems, stakeholders will have a set of decisions to make at each stage of the process.

ILLUSTRATIVE: Some open questions for identity stakeholders

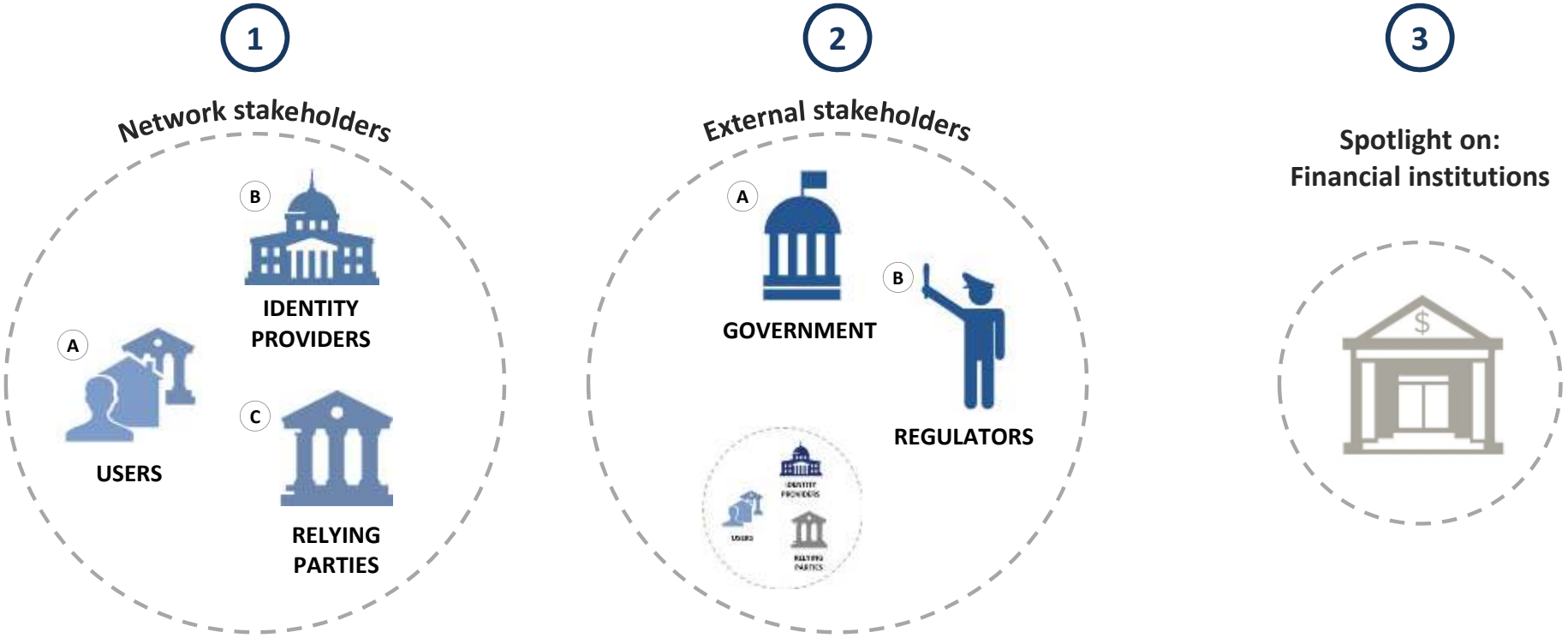
1. **Problems and user groups**
   - Which user group does this system serve? What problems will the system solve?
   - What unique characteristics will affect this user group's acceptance and use of an identity system?
   - Which archetype is best suited to solve this problem?
2. **Primary dimensions of choice**
   - Which entities should act as IdPs in this system?
   - What type of RPs should be included in this system?
   - What type of information must be transferred in the system?
3. **Secondary dimensions of choice**
   - What technology standard and trust framework will the system use?
   - What assurance model will the system use?
   - Should the system use an identity-as-a-service, fee-for-transaction business model?
   - How will the governance body be organized? What entities will be involved in system governance?
   - How will the user give consent in transactions?
   - Will any exceptions to user consent requirements be allowed?
   - How will the public sector be engaged in shaping the operational standards?

Benefits

The implementation of digital identity networks would benefit a set of different stakeholder groups

Identity systems that are constructed based on this guidance will deliver benefits both to the stakeholders involved directly in the identity network and to external stakeholders. FIs, specifically, would accrue deep benefit as a result of the implementation of digital identity.

STAKEHOLDER GROUPS



What benefits would accrue to network stakeholders?

Network stakeholders are parties who are involved in the core operation of the network itself. The network stakeholders are users, IdPs and RPs.

A

USERS

Privacy and control
Users are able to control who has access to their attributes

Security
User attributes are held in safe and secure locations

Convenience
Digital attribute transfer allows users to transact in an efficient manner

Transparency
Users have visibility into how and when their attributes are exposed

B

IDENTITY PROVIDERS

Revenue growth
IdPs can charge fees for processing identity transactions

Decreased risk and liability
IdPs understand their liability in the event of data loss or breach

Competitive positioning
IdPs can forge a strong relationship with users and position themselves as a critical part of the digital economy

Improved products and services
IdPs can use detailed and trusted customer information to deliver tailored services

C

RELYING PARTIES

Information accuracy
RPs have access to trusted, verified identity information

Decreased transaction abandonment
A streamlined user experience removes barriers to completing transactions

Service tailoring
RPs can provide more tailored products and services

Decreased risk and liability
RPs understand their liability in the event of data loss or breach

Service provision
RPs can differentiate between illicit and legitimate users

What benefits would accrue to users?

USERS

Privacy and control

1. Privacy and control

- Users would have full control over which IdPs hold their attributes
- Users consent would be required before IdPs could expose attributes to RPs
- User data would not be sold by third parties
- The minimum amount of user information required would be transferred during transactions

Security

2. Security

- User attributes would only be held by entities meeting system standards and requirements for information handling and storage
- Digital attribute storage would make identity information resistant to damage, destruction or loss
- Users would have the ability to disperse their identity information, creating contingency if an IdP suffered a data breach or data were erased or stolen, and reducing the impact of a data breach on the user

Convenience

3. Convenience

- Digital identity and digital attribute transfer would simplify and improve the user experience in transactions, eliminating the need for users to track multiple authentication methods (e.g. usernames and passwords) and manually submit personal information during transactions
- Attributes would be transferred digitally, removing the potential for human error and subsequent information remediation
- Users would be able to easily update information held with their IdPs and would not have to deal with transactions being executed based on inaccurate or out-of-date information

Transparency

4. Transparency

- Users would have visibility into which attributes would be exposed and to what entity during identity transactions

What benefits would accrue to users?

USERS: Case study

Estonia's e-government system protects citizen information, provides an extremely convenient experience for users and allows them to feel ownership over their data.

E-Government

Government solution, Estonia

- The Government of Estonia has created a digital interface between citizens and government agencies. The government holds citizen information in a centralized Population Registry and acts as the IdP and governing body, transferring reliable and trusted data to RPs.
- Citizens are each assigned an eID identifier that they can use to log on to the State Portal, which provides access to dozens of services, from voting, to updating automobile registries, to applying to universities. The government transfers the attribute information needed to complete each transaction from the Population Registry to the RP, and citizens are able to see what entities have accessed their information.
- Citizens of Estonia have the ability to view who has accessed their records, how often and for what purpose. This transparency allows citizens to feel ownership over their data, as they are able to see how the information is being used.
- A compelling example is the Electronic Health Record – a nationwide system that integrates data from various healthcare providers into a single portal. Users are able to log on to a Patient Portal to control their treatment and manage their healthcare information.

Chekk allows users to own, manage and share their personal information

Chekk

Private sector solution, Global

- Chekk is a mobile solution that provides users with a secure wallet of their personal attributes and allows them to share up-to-date information with the entities with which they transact.
- In the Chekk system, only the information required for a transaction is supplied, meaning that the user is in control and their privacy is protected.

What benefits would accrue to IdPs?

IDENTITY PROVIDERS

Revenue growth

1. Revenue growth

- IdPs would complete identity transactions for RPs; this would allow them to monetize identity-as-a-service through per-transaction fees or other business models

Defined risk and liability

2. Defined risk and liability

- Liability guidelines would be clearly defined and communicated; IdPs would be clear about their liability in the event of data loss or breach, or contravention of the standards for identity provision

Competitive positioning

3. Competitive positioning

- IdPs would be able to forge a strong relationship with users and position themselves as a critical part of the digital economy, given their unique insight into users and their established position of trust

Improved products and services

4. Improved products and services

- IdPs would have increased access to detailed and reliable user information that would allow them to better tailor processes, products and services
- IdPs could begin to draw on non-standard user attributes to better manage and evaluate risk (e.g. health records)
- Secure digital identity protocols and digital attribute transfer would improve user experience and expand the number of services that IdPs could securely provide online

What benefits would accrue to IdPs?

IDENTITY PROVIDERS: Case study

A set of banks act as IdPs in the TUPAS system, providing individuals with access to over 180 public and private services.

TUPAS

Private sector solution, Finland

- The Federation of Finnish Financial Services drove the creation of a bank identity system called TUPAS, designed to improve user access to online services.
- The RPs pay for the service (initiation fees, monthly fees and fees for set transaction volumes). Users may also be charged on a monthly basis, depending on their relationship with their bank.
- While a group of telecoms in Finland offer a competing service, as of February 2016, 95% of all online service logins were processed through TUPAS. Only 2% of online service logins were processed through the competing system. This may be due to the government's strong adoption of TUPAS, citizen loyalty towards government and banks, or the fact that it was the first successful service in the region. TUPAS has established a new revenue stream for banks as well as a strong competitive position.
- With most banks, the user must approve and certify that the data being transferred from the bank to the RP are accurate, eliminating any liability risk for the IdP.

What benefits would accrue to RPs?

RELYING PARTIES

Information accuracy

1. Information accuracy

- RPs would have access to trusted, verified identity information matched to the level of assurance required for their products or services; this would eliminate the need for information remediation and for information cross-checks through paid third-party services
- Digital attribute exchange would eliminate the potential for human error in transactions

Service tailoring

2. Service tailoring

- RPs would be able to provide more tailored products and services to users by requesting access to identity information beyond what they would traditionally require to complete transactions

Service provision

3. Service provision

- More reliable and accurate identity protocols would give RPs greater ability to differentiate between illicit and legitimate users, and to deny or provide services accordingly

Decreased transaction abandonment

4. Decreased transaction abandonment

- A more streamlined user experience would remove barriers to completing transactions (e.g. forgotten login information, required account creation, rejected billing information) and would therefore reduce the rates of users' transaction abandonment

Decreased risk and liability

5. Decreased risk and liability

- Liability guidelines would be clearly defined and communicated; RPs would be clear about their liability in the event of data loss or breach, or contravention of the standards for identity provision

What benefits would accrue to RPs?

RELYING PARTIES: Case study

The Population Registry is a central database that stores identity information – the data are trusted by many entities in Finland as a comprehensive source of up-to-date information about citizens, assets and legal entities.

Population Registry

Government programme, Finland

- The Population Registry is a national database owned and maintained by the Finnish government. The government acts as the IdP, transferring attributes to public and private RPs.
- Citizens are required to provide up-to-date information to the Population Registry, such that IdPs can trust that the information they are receiving is accurate.
- Public RPs that require attributes to complete transactions can use citizens' national ID numbers to access data held in the Population Registry. The necessary attributes are transferred digitally from the registry to the RP.
- Private RPs can also subscribe to the Population Registry and access information (with consent) to provide better products and services to their users.

What benefits would accrue to external stakeholders?

External stakeholders are parties that are not involved in the system's day-to-day operation, but are key stakeholders in the system. The external stakeholders are governments and regulators.

A

GOVERNMENTS

Process streamlining and efficiency
Governments can more efficiently interact with their citizens, saving time and money

Improved service delivery
Governments can more easily identify and deliver services to various groups of citizens

B

REGULATORS

Tracing of assets
Regulators can more effectively trace asset origination and ownership

Transparent view of entities
Regulators can access an aggregated view of legal entities across their hierarchies

Improved compliance
Regulators can access trusted, up-to-date attribute information for users, improving the effectiveness of the overall compliance process

Data standardization
Data collection and storage can be standardized across all FIs, reducing friction in data aggregation

What benefits would accrue to governments?

GOVERNMENTS

Process streamlining and efficiency

1. Process streamlining and efficiency

- Governments would be able to more efficiently interact with their citizens, saving time and money in the delivery of services such as tax filing and the distribution of social assistance

Improved service delivery

2. Improved service delivery

- Governments would be able to leverage accurate identity information to more easily identify the individuals and entities that are eligible to access given services
- Governments would be able to easily identify and deliver services to those who might be financially or socially excluded due to the lack of traditional identity information

What benefits would accrue to governments?

GOVERNMENTS: Case study

The Aadhaar programme was introduced in India to increase social and financial inclusion by providing identity for all Indians residents, many of whom previously had no means of proving their identities.

Aadhaar

Government programme, India

- The Aadhaar card was developed to improve financial inclusion in the country. The Unique Identification Authority of India (UIDAI) acts as the central IdP, controlling who has access to the data that they collect and store.
- To receive a card, individuals submit various documents to a local registrar. If they are unable to provide documentation, an "introducer", such as an elected representative or a local teacher or doctor, can vouch for the person's identity. This parallel process decreases the chance of UIDAI storing inaccurate information or providing social services to illegal immigrants or other illicit actors. The UIDAI has a database that holds information such as name, date of birth, and biometrics data that may include a photograph, fingerprint, iris scan, or other information.
- The Aadhaar program has been very effective in increasing financial inclusion with over 1 billion people enrolled for accounts, however there are still some outstanding concerns about information protection and privacy.

The Estonian e-Residency program allows non-Estonian citizens to gain digital residency in the country.

E-Residency

Government programme, Estonia

- The e-Residency program allows non-Estonian citizens to get a digital ID card that enables them to use Estonian private and public services and to use secure digital signatures. The purpose of the program is to create a virtual business environment and continue to position Estonia as a hub of the digital world
- Since its inception in December 2014, almost 10,000 people have applied for e-Residency and over 400 have established an new company domiciled in Estonia.

What benefits would accrue to regulators?

REGULATORS

Tracing of assets

1. Tracing of assets

- Regulators would be able to more effectively trace asset origination and ownership, increasing their ability to track the proceeds of criminal activity
- Asset rehypothecation could be traced, ensuring that assets would not be rehypothecated beyond their total value

Transparent view of entities

2. Transparent view of entities

- Regulators would have access to an aggregated view of legal entities across their hierarchies, increasing their ability to evaluate systemic risk and manage stability

Improved compliance

3. Improved compliance

- Access to trusted identity information would increase the ability of FIs to be compliant with anti-money laundering, know-your-customer and other regulations within their jurisdiction
- Access to trusted information on legal entity and asset identity would allow FIs to more accurately detect money laundering and other suspicious transactions
- Access to trusted digital attributes would allow FIs to automate their compliance processes to some degree, potentially allowing regulators to increase the required frequency of compliance reviews

Data standardization

4. Data standardization

- Data collection and storage could be standardized across all FIs, reducing friction in data aggregation

What benefits would accrue to regulators?

REGULATORS: Case study

GLEIF is an organization that supports the implementation of the Legal Entity Identifier standard – this standard might ultimately become a common thread between identifier systems in an effort to create a standardized global view of legal entities.

Global Legal Entity Identifier Foundation (GLEIF)

Non-profit organization, global

- GLEIF manages a network of Local Operating Units that issue Legal Entity Identifiers (LEIs) to legal entities worldwide.
- Legal entities engaging in financial transactions submit a standard set of attributes to a Local Operating Unit, which validates them against third-party records and then issues an LEI. GLEIF holds the master file of all LEIs and associated entity information.
- The system was introduced by financial regulators to improve micro- and macro-prudential risk assessment and management, increase market transparency and improve the accuracy of financial data.
- Beyond financial services and regulation, the goal of the LEI system is to provide reliable identity information to permit unique identification of legal entities worldwide, in financial services and beyond (e.g. supply chain applications).
- Over 430,000 LEIs have been issued since October 2015. The LEI is intended to become the link between all other identifier systems (e.g. know-your-customer systems, business register codes, etc.). This would allow regulators to have a consistent and comprehensive view of all legal entities and financial instruments globally.

FIs have key features that would give them structural advantages within identity systems

FIs have unique advantages that make them well-suited to playing key roles in digital identity networks.

ADVANTAGES OF FIs IN DIGITAL IDENTITY

FIs are highly reliant on identity

Identity is central to the function of FIs, while they bear a large part of the cost of ineffective identity protocols

FIs are connected to many key identity stakeholders

FIs have standing relationships with users, governments, regulators and other key stakeholders, and have experience working with these groups on key concerns while balancing competing interests

FIs are trusted institutions

FIs are more trusted by consumers to hold personal information than other institutions, such as governments, telecoms and technology companies

FIs have existing business models that do not require directly monetizing customer information

CASE STUDIES

iDIN

Private sector solution, Netherlands

iDIN was created to capitalize on the large investments that banks have made in onboarding their customers; banks already collect highly trusted identity information and are well positioned to transfer it to other parties.

NemID

Private sector solution, Denmark

To maximize the adoption of NemID, the governing body wanted to cooperate with private actors who have frequently used services; banks not only interact with individuals on a regular basis, but are also seen as trusted institutions that already store user identity.

SecureKey Concierge

Public-private programme, Canada

SecureKey partnered with nine banks that are trusted and hold accurate data; this data can be used to authenticate individuals in the system.

What benefits would accrue to FIs from the implementation of digital identity?

The benefits to FIs of implementing digital identity fall into six categories:

FINANCIAL INSTITUTIONS

Improved products and services
FIs will be able to use detailed and trusted customer information to deliver tailored services to customers

Operational efficiency
Digital attribute transfer and handling will allow FIs to streamline and automate many processes, eliminating human error

Decreased fraud
The secure, digital storage of user information will reduce fraud resulting from stolen information or compromised authentication

Improved compliance
Digital attribute handling and greater access to user identity will allow FIs to complete compliance processes more easily and accurately

Revenue growth
FIs will have the opportunity to increase revenue from improved products and services as well as to offer identity-as-a-service

Better user experience and competitive positioning
FIs can offer a streamlined user experience and position themselves as a critical part of the digital economy

What benefits would accrue to FIs from the implementation of digital identity?

FINANCIAL INSTITUTIONS

Improved products and services

1. Improved products and services

- FIs would have increased access to detailed and reliable user information that would allow them to better tailor processes, products and services such as:
  - Risk scoring for insurance products
  - Financial advisory
  - Asset management
  - Credit scoring
  - Loan adjudication
- FIs could begin to draw on trusted information, with consent, to better manage and evaluate risk; secure digital identity protocols and digital attribute transfer would improve user experience and expand the number of services that FIs could securely provide online

Operational efficiency

2. Operational efficiency

- FIs would be able to access user information in a consolidated, digital form through queries in the digital identity network; having attributes in a consolidated digital form would provide a single view of the customer and allow FIs to streamline customer-facing operations, such as onboarding, as well as many back-end processes
- Digital identity for assets would allow FIs to track financial products and assets more closely, through greater visibility into ownership and the resolution of rehypothecation concerns

Decreased fraud

3. Decreased fraud

- User information would be held only by entities that follow standards around data protection; this would reduce fraud (such as card-not-present transactions made using shipping and billing information stolen in large-scale data breaches)
- Digital authentication methods would reduce fraud resulting from hacked or compromised user accounts

What benefits would accrue to FIs from the implementation of digital identity?

FINANCIAL INSTITUTIONS

Improved compliance

4. Improved compliance

- Digital identity would give FIs access to trusted, up-to-date attribute information for users, improving the accuracy of know-your-customer processes
- Digital information transfer and storage would allow FIs to complete their compliance processes more quickly and easily, allowing faster processing and reducing time spent on information remediation and correcting human error
- Compliance processes could be automated and executed on more regular cycles
- Digital identity would give FIs better visibility into corporate ownership structures and the identity of corporate directors to improve corporate know-your-customer processes
- Digital identity would give FIs better visibility into asset origination and ownership

Revenue growth

5. Revenue growth

- FIs could monetize identity-as-a-service through business models such as subscription fees with RPs or fee-for-transaction services for high-assurance identity transactions, including:
  - Authentication
  - Digital signatures
  - The completion of identity transactions for RPs, such as providing attribute information (e.g. providing shipping information to merchants) or providing information about attributes (e.g. attesting to a merchant that a user is over a certain age based on date of birth)

Better user experience and competitive positioning

6. Better user experience and competitive positioning

- By collaborating with governments, public sector entities and other private sector entities, FIs would become part of a trusted ecosystem working on developing the digital economy
- As trusted safeguards of user information, FIs would increase the strength of their relationships with users

What benefits would accrue to FIs from the implementation of digital identity?

FINANCIAL INSTITUTIONS: Case studies

Aire is able to assist individuals who lack traditional credit information by using non-traditional user attributes to build a new credit score.

Aire

Private company, United Kingdom

Aire, a UK-based start-up, offers an alternative to traditional credit-scoring techniques. Aire allows individuals to submit a wide range of materials that are used to evaluate the individual's creditworthiness; for example, a user could submit utility or Netflix bills.

Know-your-customer utilities provide FIs with access to trusted, up-to-date attribute information for users, improving the accuracy of individual and corporate know-your-customer processes.

Industry Know-Your-Customer Utilities

Private solutions, global

Industry know-your-customer utilities, such as Thomson Reuters' OrgID or DTCC's Clarient Entity Hub, are intended to serve as reliable repositories of identity information on legal entities, eliminating the need for entities to perform know-your-customer requirements on their counterparties in financial transactions and giving them access to reliable and current information.

FIs in the TUPAS system are the only entities to hold and transfer user information, allowing them to monetize identity-as-a-service through business models such as subscription or fee-for-transaction services with RPs.

TUPAS

Private sector solution, Finland

In the TUPAS system, RPs must pay IdPs (in this case, a consortium of banks) to access trusted and accurate user attributes.

Future-State Applications

Digital identity offers FIs improved and new capabilities

Beyond the first-level benefits of digital identity that FIs would receive as a result of participating in an identity system, we have explored some future-looking use cases that illustrate additional capabilities that digital identity might offer to FIs.

POTENTIAL FUTURE-STATE APPLICATIONS

1. Tailored risk profiles

2. International resettlement

3. Attributes tied to payment tokens

4. Digital tax filing

5. Determining total risk exposure

6. Identifying transaction counterparties

7. Linking individual identity to corporate identity

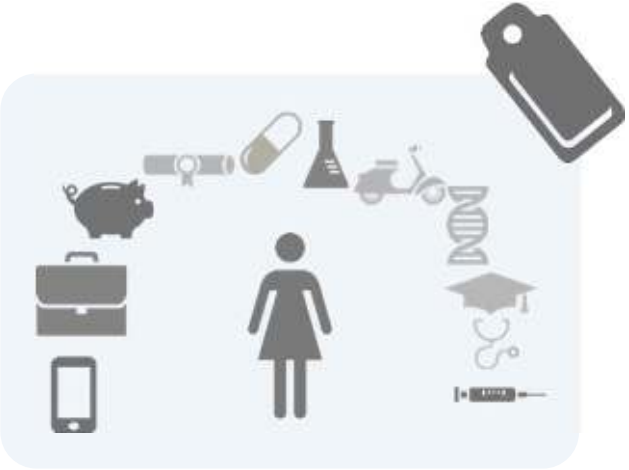
8. Tracking total asset rehypothecation

What additional capabilities can digital identity offer to FIs?

1. TAILORED RISK PROFILES

CURRENT STATE:
FIs currently create risk profiles for individuals and legal entities using the limited information that is collected when customers are onboarded and predictive algorithms to provide relevant and tailored products and services to their customers.

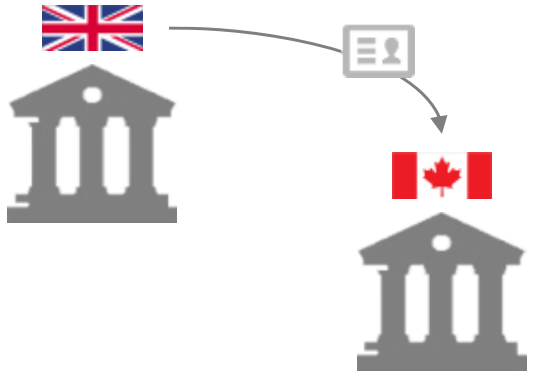
HOW WOULD DIGITAL IDENTITY HELP?
FIs could leverage trusted user attributes, with a user's consent, to more effectively build risk profiles for their customers and therefore tailor credit- and risk-based products. This enhanced user experience would ultimately lead to increased customer stickiness and offer growth opportunities for FIs.



2. INTERNATIONAL RESETTLEMENT

CURRENT STATE:
Today's onboarding processes require every FI to onboard a customer from a zero-knowledge state, resulting in difficulty opening accounts for entities that are unable to prove their identities, and disregard of financial history.

HOW WOULD DIGITAL IDENTITY HELP?
Users could transport their digital identity across jurisdictions and use it to easily gain access to financial and other services in their new place of residence; the attestations and attributes held by the user's original FI(s) would serve as the basis for new FIs to become IdPs. This would eliminate the need for the recipient FI to perform the costly and labour-intensive know-your-customer process that would otherwise be required. In addition, it would reduce the time and effort needed for FIs to onboard users, and allow them to incorporate trusted, historical information.



What additional capabilities can digital identity offer to FIs?

3. ATTRIBUTES TIED TO PAYMENT TOKENS

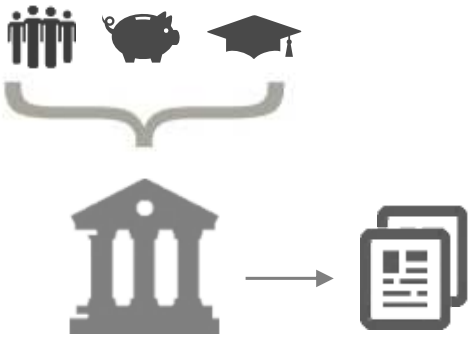
CURRENT STATE:
When completing transactions, customers are required to manually provide their attributes (e.g. confirmation of age, shipping information) or proof of attributes to merchants at the point of sale.

HOW WOULD DIGITAL IDENTITY HELP?
FIs could automatically provide customer attributes to merchants, streamlining and securing the transaction process for the merchant and customer. The digital transfer of attributes would eliminate the potential for human error in information transfer and dramatically reduce information remediation and transaction abandonment for the RP.
Note: This automatic transfer of attributes could be supported by an additional factor of authentication (e.g. mobile or behavioural authentication) to prevent fraud.

4. DIGITAL TAX FILING

CURRENT STATE:
Individuals and businesses currently file their taxes based on the aggregation of pieces of information from multiple sources (e.g. FIs, employers, educational institutions, etc.).

HOW WOULD DIGITAL IDENTITY HELP?
In collaboration with governments, taxes could be automatically completed and filings generated by customers' chosen FIs, using their complete knowledge of customers' financial holdings, assets, income and personal circumstances. With user consent, all of this information would be available through a robust digital identity network. This would allow the typically complex and tedious tax filing process to be completed efficiently and accurately.

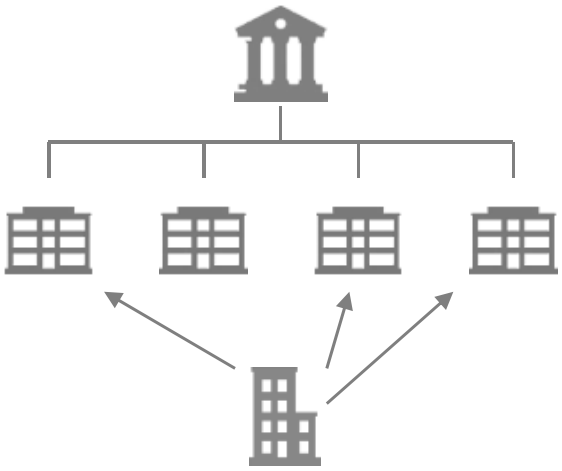


What additional capabilities can digital identity offer to FIs?

5. DETERMINING TOTAL RISK EXPOSURE

CURRENT STATE:
Legal entities are often unable to determine their total risk exposure to a given counterpart due to complicated ownership structures and difficulty aggregating a complete view of a legal entity.

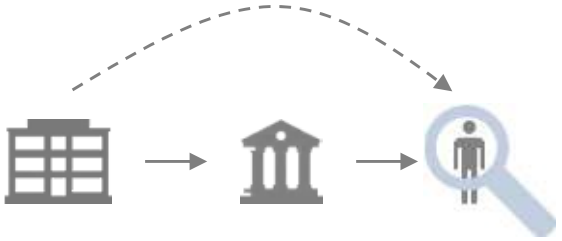
HOW WOULD DIGITAL IDENTITY HELP?
Transaction counterparties could have a consolidated view of the corporate structure of the entities with which they are transacting, allowing them to determine their total risk exposure to that entity across transactions and lines of business.



6. IDENTIFYING TRANSACTION COUNTERPARTIES

CURRENT STATE:
It is currently challenging or impossible for entities to identify all entities that are participating in a given transaction; they may not have visibility into the end customer in a transaction that is being completed by a broker or other counterparty.

HOW WOULD DIGITAL IDENTITY HELP?
Legal entities could request visibility into the consolidated identity of a third party and the ownership history of a given asset involved in a transaction. This would allow them to identify both the direct customer and the end customer in the transaction, better informing the decision of whether to complete the transaction.

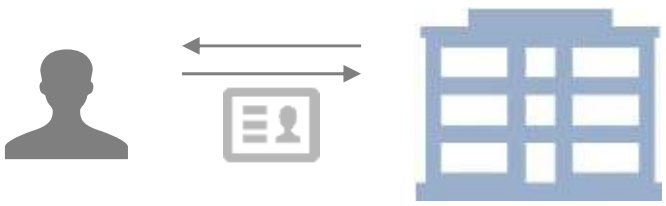


What additional capabilities can digital identity offer to FIs?

7. LINKING INDIVIDUAL IDENTITY TO CORPORATE IDENTITY

CURRENT STATE:
Individual and corporate identity information is currently not linked; it is challenging to identify individuals who are associated with corporate entities.

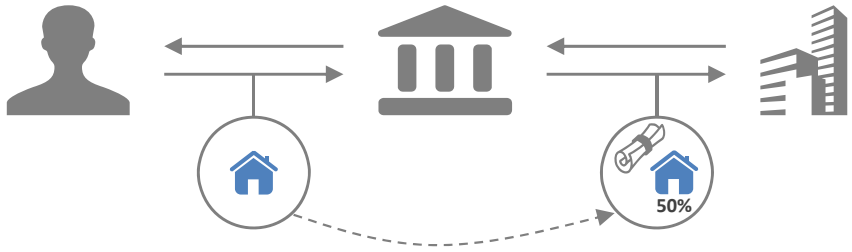
HOW WOULD DIGITAL IDENTITY HELP?
The digital and standardized collection, storage and transfer of attributes for both individuals and legal entities would ensure identity information is accurate and up-to-date. Linkages between these systems would create reliable pictures of the identities of individuals affiliated with legal entities for know-your-customer and other purposes.



8. TRACKING TOTAL ASSET REHYPOTHECATION

CURRENT STATE:
The transaction and ownership history of assets can become ambiguous as assets are rehypothecated; this exacerbates counterparty risk and asset valuation uncertainty, while the lack of a historical tracking mechanism prevents the enforcement of limits on the extent of asset rehypothecation.

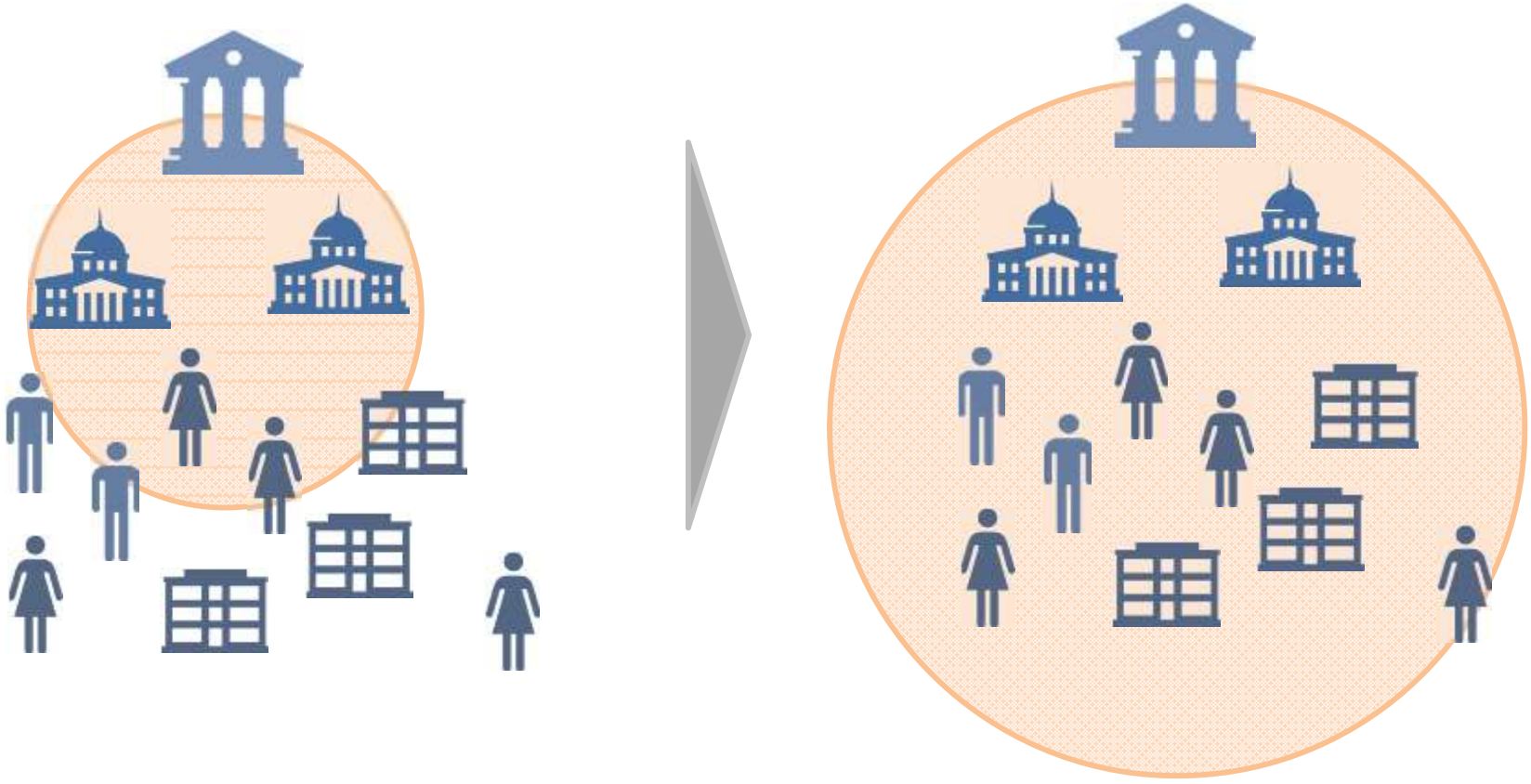
HOW WOULD DIGITAL IDENTITY HELP?
Consolidated, standardized and digital identity information for assets would be available to all entities engaging in a transaction involving that asset, giving transaction counterparties the ability to check asset information, such as issuer and transaction history; this would enable the tracking of the asset ownership structure and composition, and prevent over-rehypothecation due to the lack of visibility into past transactions involving that asset.



Implementation of Identity Systems

Implementation of a digital identity system should follow a bottom-up approach

We have outlined our perspective on the prime movers within digital identity solutions and how they should implement digital identity solutions. It is critical to observe that this is the first step in a bottom-up approach that would result in systems being scaled outwards to incorporate greater numbers of users, relying parties and identity providers as guidelines and functionality are tested and refined.



The system is launched with a critical mass of parties to test and refine

The system is scaled to increasing numbers of users, relying parties and identity providers

Global identity will never exist as a monolith

This document has laid out a principles-based approach to building effective, sustainable and bounded natural identity networks as the foundation for interconnecting individual identity networks. There will never be a single, global solution for identity.

Identity serves different needs

Different user groups have different needs and requirements for identity. Identity systems for individuals are designed to increase the ability of users to perform transactions in a safe and secure manner. Identity systems for legal entities are intended to enable comprehensive aggregation at a macro level – whether to determine total exposure to a single legal entity or manage systematic risk and stability. Identity systems for assets are designed to allow tracking and provide transparency around ownership and value. Privacy is one of the key requirements of individual identity, but is much less important in legal entity and asset identity and may even interfere with the larger purposes of these systems. Individuals have self-determination, whereas legal entities and assets have custodians who act on their behalf.

Identity is cultural

Identity is hugely affected by cultural and geopolitical factors. For example, while some populations are comfortable having a national ID card, this system has failed in other jurisdictions. Certain authorities may not be a stable government to drive the creation and adoption of digital identity.

This means that, aside from having different configurations for purely practical reasons, identity systems will differ dramatically to suit the cultural and geopolitical needs that they serve.

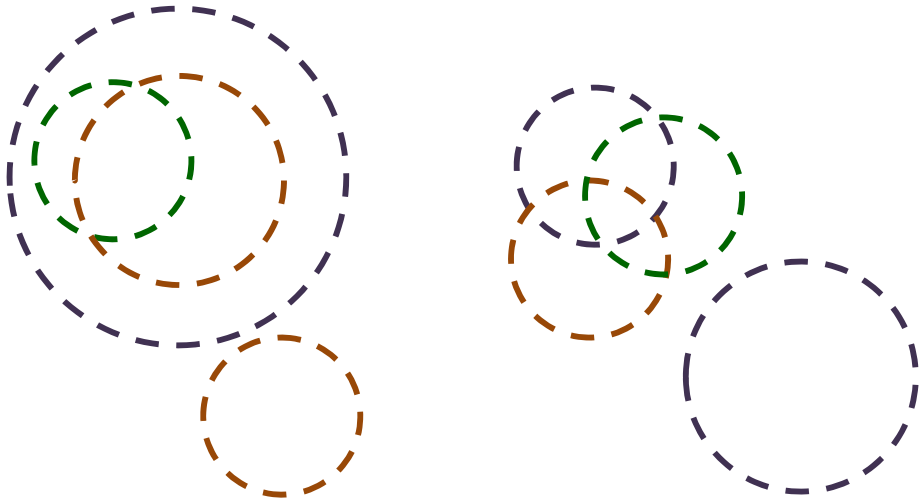
There is no one-size-fits-all for identity.

A global system for identity therefore initially requires the construction of discrete identity networks, and then the creation of rails between them

Creating a global solution for identity is a two-step process: the key to building a global system for digital identity is first building successful natural identity networks that address the unique needs and preferences of their user group and situation, and then building connective tissue that creates interoperability between these systems.

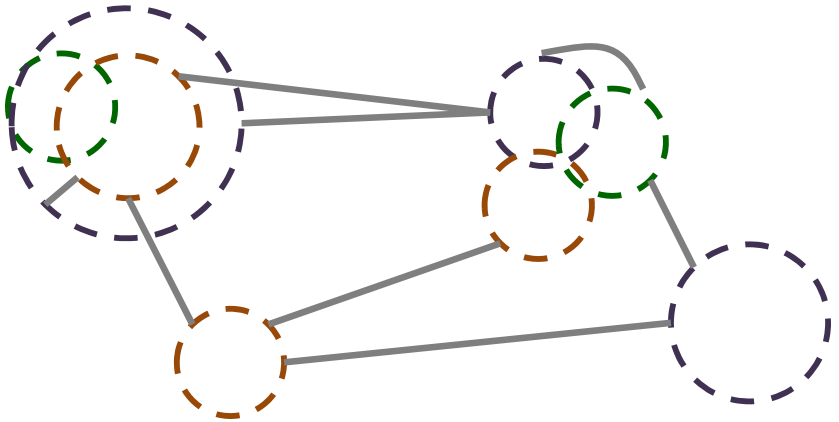
1
Implementation: Configuring natural identity networks

The configuration of natural identity networks will be guided by the decisions made against the primary and secondary dimensions of choice



2
Interconnection: Building the rails for global identity

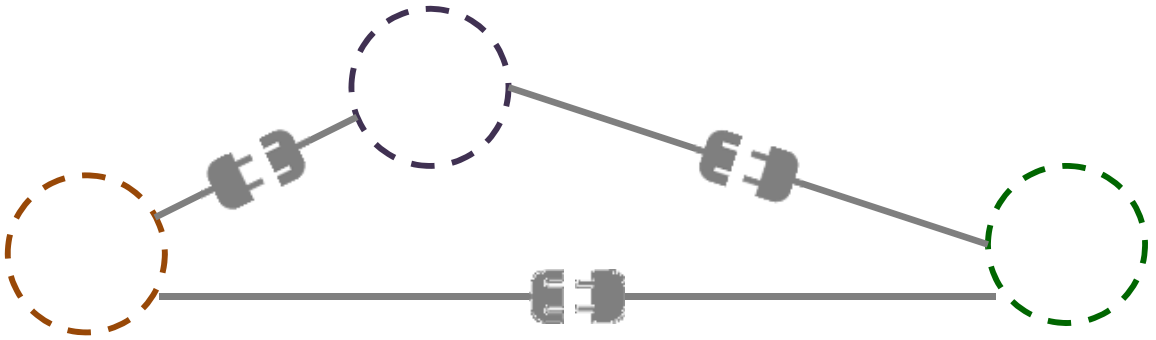
Building the rails between natural identity systems will create global interconnection and interoperability



While the rails for global identity will begin to emerge as systems develop, it is important that entities follow a guiding framework

Building identity as a two-step process enables identity systems to be built by narrowing the required stakeholders to groups that have similar needs and concerns, and therefore have relatively aligned incentives. It also ensures that these systems are tailored to the specific needs and wants of their user and stakeholder groups and will therefore gain the uptake that a top-down, one-size-fits-all system would not attain. However, these solutions should also be built following a common framework that will ensure interoperability by defining the features, attributes and requirements of the identities that are exchanged in the system. This reinforces the need for individual identity systems to be built by entities such as financial institutions that have experience working together to define standards, and then building individual systems within these standards.

Implementing discrete digital identity systems that suit the unique needs and cultural factors of users in their own jurisdictions, and designing these systems around resilience, interoperability and interconnection, will allow a global blueprint for digital identity to emerge.



There are many standing questions and uncertainties that must be considered in the creation of new identity systems

SOME THOUGHT STARTERS TO BUILDING IDENTITY SOLUTIONS

Drivers of identity systems will need to consider many detailed tactical questions in the configuration and implementation of their own identity solutions. We have provided some example questions and uncertainties below.

- Which entities need to be involved in an identity system for your area and user group – governments, regulators, financial institutions, consumer groups, others?
- What business model that will be sustainable in that situation – user pays, relying party pays, government pays? By transaction, subscription, subsidized through other services?
- What governance structure is necessary for the system – who should be involved, what should be the extent of their mandate, how will governance be renewed and refreshed?
- What is the minimum viable identity product required for that situation – what users should be involved, what services need to be covered, which entities should be involved, what metrics are being tested?
- Which frameworks and standards can be adopted for the identity system?
- Which components of the identity stack must be proprietary, and which ones can be outsourced or obtained through partnership?
- What technology platform is required for the system?
- What is the best method of communicating system functionality and benefits to users?

Contact Details

For additional information, please contact:

WORLD ECONOMIC FORUM CORE PROJECT TEAM

R. Jesse McWaters
Project Lead, Financial Services
World Economic Forum
Jesse.McWaters@weforum.org

Giancarlo Bruno
Senior Director, Head of Financial Services
World Economic Forum
Giancarlo.Bruno@weforum.org

PROFESSIONAL SERVICES SUPPORT FROM DELOITTE

Christine Robson
Deloitte Canada
crobson@deloitte.ca

Rob Galaski
Deloitte Canada
rgalaski@deloitte.ca

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD