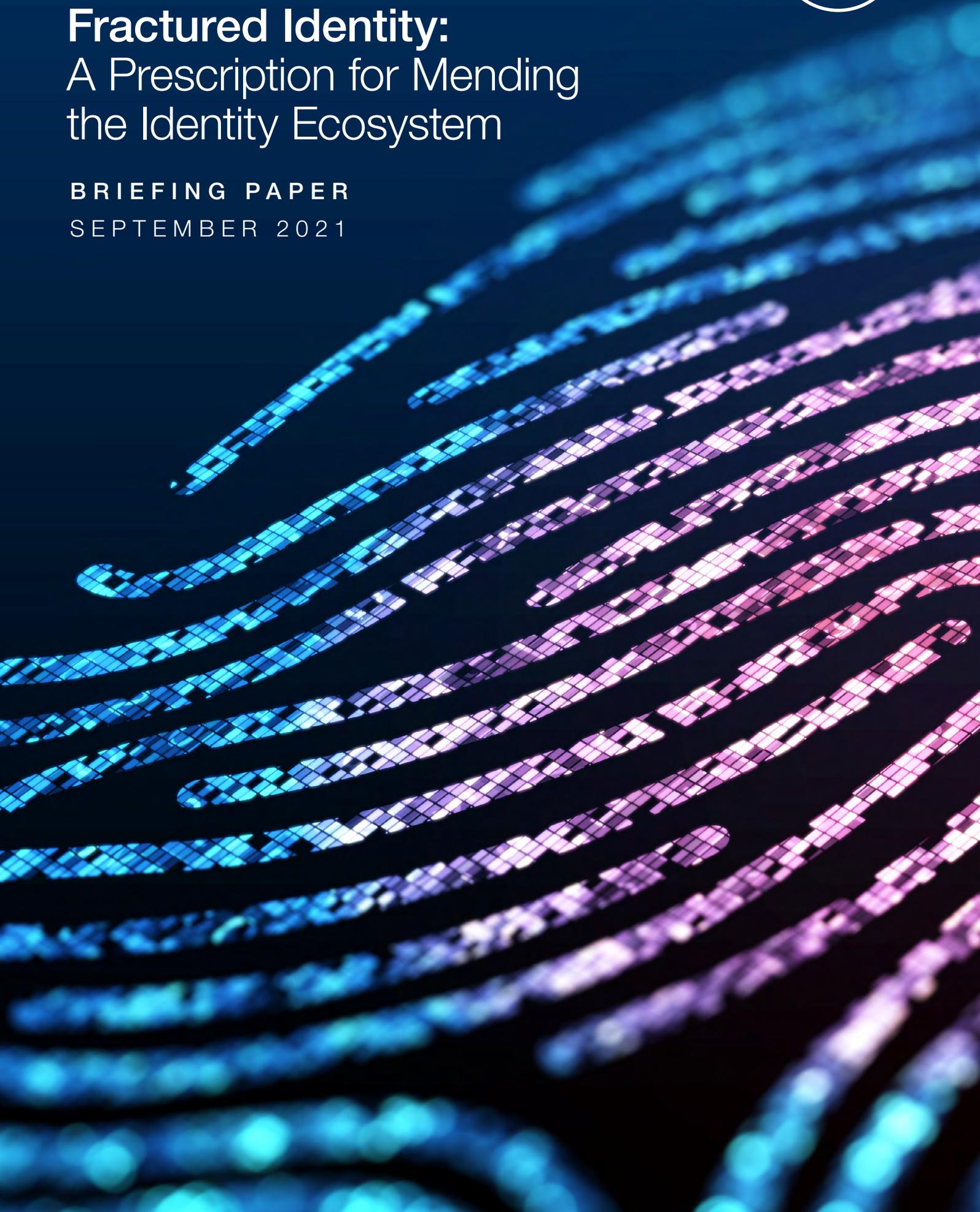


Fractured Identity: A Prescription for Mending the Identity Ecosystem

BRIEFING PAPER
SEPTEMBER 2021



Contents

3	1 Introduction
5	2 Principles of Digital Identity
6	3 The Components of Digital Identity
7	4 Elements of Trust
8	5 Putting Trust into Practice
10	6 Obstacles for the Digital Identity Ecosystem and Next Steps
12	Conclusion
12	Acknowledgements
12	Endnotes

Disclaimer

This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

© 2021 World Economic Forum. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.



As we emerge from the COVID-19 pandemic, some deficiencies in public infrastructure have been laid bare. Specifically, methods for verifying identity to distribute benefits and manage services in many cases were proven inadequate. Individuals were unable to apply for benefits or conduct other transactions in-person, and the rapid transition from face-to-face services to digital services often resulted in a proliferation of fraud.¹ For example, the United States Department of Labor estimates that at least \$36 billion in COVID relief unemployment was lost to improper payments, mostly from fraud in fraudulent unemployment claims.²

Throughout the pandemic, the lack of consistent and interoperable approaches to assert identity digitally further impacted the ability of governments to rapidly, and effectively, build applications to track and manage both testing and vaccination. This forced constituents and providers to use less convenient and less trustworthy analogue methods for managing high-risk, pandemic-related transactions. Digital identity – the representation of a unique individual engaged in a digital transaction – is central to managing fraud risk and improving accessibility of online transactions.

Globally, digital identity is fragmented. Historically, countries have defined their own digital identity requirements, data, attributes and policies. In some countries, individuals are issued with a smart card, which can be used for a variety of public and private sector transaction; in other countries, an individual can have multiple credentials to access different local and state resources; and still in others, there may be nothing at all at this time. This localization is a substantial challenge, with governments and private sector organizations executing on disparate identity schemes across geographies to enable relying parties to have confidence in a credential or attribute. Passports have always had a high level of trust and standardization but there is not yet a digital equivalent. The idea that each of these disparate localities will align on a single paradigm is flawed. Instead, to coalesce an international ecosystem, specific roots of trust can be established to enable technical and policy interoperability between and among digital identity systems.

A strong, global identity ecosystem has the potential to improve digital transactions for government, commercial organizations and individuals:

- Government: While some would want to see the role of government in digital identity limited, it often has a role as both an identity provider and a relying party. In most cases government is the entity that issues those foundational documents – birth certificates, social security number, driver licences, passports – that are used to build a digital identity. A strong digital identity is an enabling force for digital transformation in the public sector and has the potential to reduce fraud, increase accessibility and decrease costs.
- Commercial: Most often commercial groups are likely to play multiple roles in an identity ecosystem as relying parties for digital identity solutions, but some organizations – financial services, telecommunications – could also be the identity providers. Digital identity can reduce fraud for commercial entities and enable easier access to services as individuals won't have to remember individual account information for each business. They can also be differentiating services that drive revenue and increase access to critical customer demographics or clients.

- Individuals: Digital identity can improve access for individuals to a variety of resources while, in many cases, also empowering them to manage their own identity and attributes. Instead of the 100+ accounts they deal with now, they would have one strong identity protected by multi-factor authentication – biometrics, mobile device, token, or all the above – to access services. In the world of a global identity ecosystem an individual could potentially use this credential to book an airline ticket, get through airport security, pass through customs and border at arrivals, and then check into a hotel.

A number of obstacles must be overcome to enable a globally interoperable digital identity ecosystem. This paper will look at those blockers and help guide policy-makers in how they could overcome them, as well as looking at the core roots of trust that enables digital identity. This paper will also focus on defining common components trust that enables a broad identity ecosystem and is, therefore, intended for global decision makers at all levels who can influence change to digital identity systems.

BOX 1 The complex role of biometrics in digital identity

It has almost become the de facto standard: either place your finger on a sensor or look at your smartphone and it unlocks giving you access to data and transactions. Since 2013, phone manufacturers have enabled individuals to use biometrics to unlock their devices. Nowadays, most people don't give a second thought to using the technology for a variety of everyday transactions.

And while people use facial recognition to verify payments from mobile devices, their use in the broader digital identity ecosystem is more complex. A common use case for enabling high-assurance digital identity on mobile devices calls for individuals to take a photo of their passport or driver licence. Security features on the document are checked as well as the biographical information.

The individual then takes a "selfie" to match against the photo on the document along with testing for

"liveness" to prevent spoofing. Sometimes the photo can also be validated with the original document issuer. While this workflow can offer a fairly high level of assurance, the systems are sometimes subject to challenges with user experience/system performance. These can lead to false rejects, requiring the individual to take additional steps that may lead to abandoning the transaction.

These systems are improving with each release but may still – along with privacy concerns – pose an obstacle for issuance of high-assurance digital credential in a remote setting. Additionally, while not the same as biometrics used for surveillance, those used in identity systems must nonetheless be deployed to align with an emerging set of privacy and regulatory regimes (e.g., California Consumer Privacy Act, EU's General Data Protection Regulation) and align to core principles such as consent and notice.

2

Principles of Digital Identity



Trust is at the core of digital identity. But other principles can guide the creation of systems that can be deployed in a trustworthy manner and in a way that promotes [broad interoperability, user adoption and organizational acceptance](#). It is important to note that these principles are not intended as directives or requirements but guiding concepts to inform the development of digital identity systems, standards and policies that can be more easily accepted across international boundaries – even if not universally implemented in their entirety.

- Digital identity services should be flexible and adaptive. Services should support the rapid integration of different end-user devices and authentication mechanisms—such as biometric technologies and low-friction solutions like behavioural analytics—based on evolving technologies and the shifting threat environment.
- A broader digital identity ecosystem will likely emerge where verified information is consumed. For example, a citizen may establish reputational trust around their digital identity that is used to post online information or receive threat alerts, such as compromised email addresses or other information that may be shared among organizations in the ecosystem.

- Strong digital identity systems should enable bi-directional trust. That is, governments need to know that authorized citizens are accessing services and information. But citizens also need to trust that they are interacting with a legitimate service, that their personal information will be protected and that they can efficiently access services.
- Digital identity systems must protect user privacy and data. When citizens and consumers interact with digital identity systems and relying parties, their attributes and data need to be appropriately protected. Providers of identity services should not seek to intercept, retain or cache them for purposes unknown and unconsented to by the citizen.
- Digital identity solutions should be user controlled and portable. This means citizens and consumers can easily access many online services with the same secure digital identity and not be locked into specific vendors and identity service providers. Governments and private entities should seek to provide individuals with choices for the digital identity solutions they wish to leverage in each transaction.

The Components of Digital Identity



In order to establish a trusted digital identity, certain components and processes must be put in place by service providers. Collectively, these processes can be applied to different use cases to mitigate risk to varying degrees. The components of digital identity include:

- Identity proofing: This is where the individual proves they are who they claim to be. This can be done in many ways but advances in this area enable individuals to take photos of their passports or driver licences and enable them to be verified and validated with the issuing authority.
- Digital identity creation and binding: After the identity is proofed, a credential is issued and bound to the individual. A popular option for credential issuance is a mobile device and it can be bound by a biometric match, such as facial recognition.
- Verifiable attributes: An alternative to traditional credential issuance is the issuance of verified attributes by an authoritative appropriate entity or organization. An individual is still identity-proofed but then has verified attributes they can assert for different transactions. The attributes are stored on a mobile device, asserted and then verified on a blockchain or other repository by the relying party.
- Authentication: This step enables an individual to open the front door of a service. Usernames and passwords are the de facto standard but multi-factor authentication via biometrics or mobile device is becoming more common.
- Authorization: Once an individual is in the front door and has been authenticated, authorization defines what they can do once in the building. For example, an individual might be able to read certain information but not have the ability to download or edit that information.
- Revocation: Digital identity solutions need to be able to support the ability for credentials and verified attributes to be revoked or invalidated. This can be executed by identity providers, attribute providers, or even individuals themselves. It is an essential capability to prevent fraud, preserve privacy and effectively manage access if a credential or attribute is compromised, expired, or otherwise changed.

4

Elements of Trust



Trust is not simple. In an identity ecosystem, trust is multi-layered. There's the trust between an individual and a credential provider, between a credential provider and a relying party, between an individual and the relying party, to name a few.

While common principles and a core understanding of digital identity components constitute a substantial step toward establishing trust, five elemental trust items are:

Category	Name	Description
Technical	Open standards	The International Organization for Standardization (ISO), the World Wide Web Consortium (W3C), The Open Identity Foundation, Trust Over IP, and the Institute of Electrical and Electronics Engineers (IEEE) are just some of the international standards organizations working on digital identity standards. Consensus-based standards organizations provide the foundational elements for a global digital identity ecosystem.
Policy	Trust frameworks	These are the business, legal and technical rules for digital identity systems. The trust frameworks lay out the rules and procedures that identity providers and relying parties must follow and who is liable if the rules are not adhered to.
Technical	Technical protocols	These protocols make sure that the digital identity systems are speaking the same language.
Policy	Certifications	Once all the pieces of an identity system are decided upon, it's a good idea to have them tested and certified. This makes sure they will work down the road and lead to fewer technical complications.
Policy	Authoritative data	Relying parties (e.g., online merchants) need assurance that the information contained in an attribute claim is correct based on where the data comes from. The veracity of an attribute is also dependent on the data source; for example, an attribute from a driver licence issuer should be given more credence than one from an online retailer.

5

Putting Trust into Practice



As the global digital identity ecosystem is still on the horizon, there are potential use cases that adhered to the roots of trust mentioned above. Any one of these uses cases has the potential to serve as the foundational identity for global interoperable identity.

- Mobile driver's licence (MDL): The MDL standard (ISO18013-5) is expected to be finalized in 2021 after four years of development. This mobile credential can be issued either in person or remotely with binding via facial recognition biometrics. Certification programmes exist that test interoperability of MDLs between different vendors and the specification has the promise to bridge the physical world with the digital. International acceptable of MDLs may be the first step in coalescing a digital identity ecosystem.
- Digital travel credential: The International Civil Aviation Organization (ICAO) is a United Nation's organization charged with creating and maintaining the standard for passports. In the early 2000s it created the standard that places contactless smart card chips in passport books.

Now the organization is creating a standard that would enable the passport to be placed on a mobile device as a digital travel credential. Mass issuance and adoption of an ICAO-standard digital travel credential could be a step forward in the creation of a global digital identity ecosystem if it could be used for something other than travel.

- Health passports: As the world emerges from the COVID-19 pandemic there is a rush to provide mobile credentials that can be used to share test results or proof of vaccination. Various organizations are working to create standards that would enable international acceptance of these credentials. Currently, the ecosystem is fractured with various organizations, countries and jurisdictions creating different solutions. It's possible the World Health Organization or another international governing body may suggest a standard to electronically prove vaccination or test results, but the market is fragmented.

BOX 2 | Adapting to different digital identity models

Digital identity is not a one-size-fits-all approach. Countries across the globe take different views on how to best achieve a digital identity model. For the most part, digital identity models are still centralized – an identity provider issues an identity that can be used at relying parties – think of passports and driver licences.

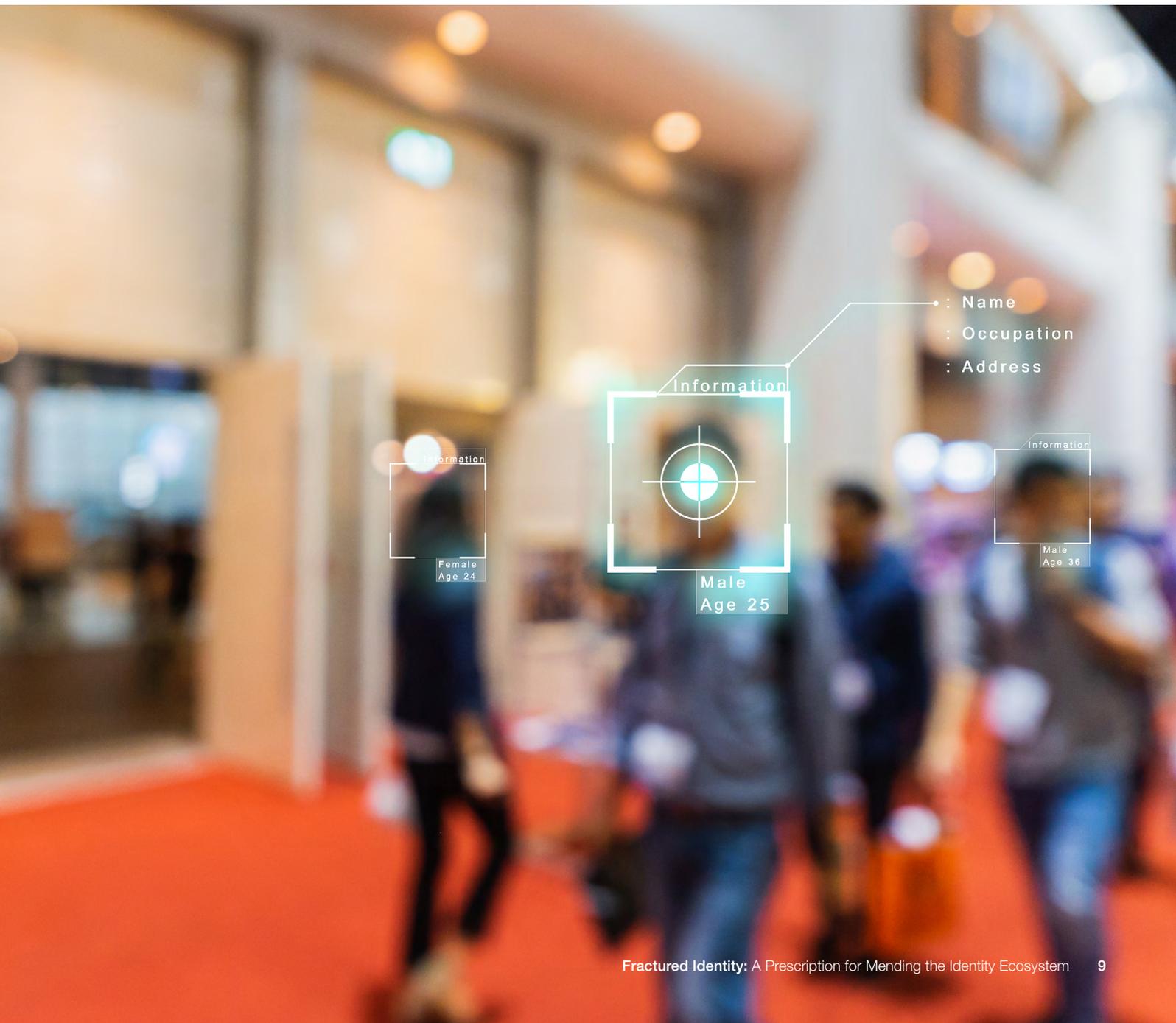
The downside of the centralized identity model is the user has little control. It's typically a one-size-fits all approach. For example, if you're trying to purchase age-restricted products, the person checking your identity can also see your specific date of birth, address and ID card number.

This model has worked in many use cases and may continue to be the dominant model for many regions, but disruptions to this traditional paradigm are emerging. Self-sovereign identity (SSI) and similar decentralized identity models are somewhat new concepts that put the individual in control

of their identity and attributes. This model sees a provider issue verified attributes that the individual can assert as needed, putting the individual in control over what and where the information is shared. Once the attribute is asserted to a relying party it is verified on a blockchain. In the same use case as above, the decentralized model of digital identity would enable an individual to show an identity that would simply state that the person was old enough to purchase the products.

Although SSI enables the individual to have greater control over where their information is shared, it has yet to gain widespread use.

This document does not propose a single approach – decentralized, SSI, or centralized – as preferable to another. Instead, it acknowledges jurisdictional differences and focuses on how to establish trust between systems and create international interoperability to the extent possible.



6

Obstacles for the Digital Identity Ecosystem and Next Steps



The obstacles for digital identity are varied. For almost 20 years, identity programmes have been attempted with varying degrees of success outside national identity programmes or some financial services offerings. There have been several impediments to widespread digital identity over the years, including the following:

- Regulation: This has been a standing issue as existing regulation on access to some information proves a hindrance. For example, in the US most states cannot share driver licence data beyond proof to operate a motor vehicle. Regulations that protect this data but enable it to be used for other purposes would greatly facilitate a digital identity ecosystem.

[Recommendation: Wide support should be given to a Task Force to Evaluate Regulatory Blockers to digital identity adoption that would](#)

[make recommendations for remediation. This may include looking at how the EU Data Governance Act is impacting identity ecosystems.](#)

- Liability: Who pays if someone makes an error? This goes back to the trust framework and who is responsible for the various aspects within a digital identity system. These systems can often get sidetracked or derailed over the discussion of who is liable.

[Recommendation: Further study is needed into how liability operates in digital identity schema and the steps that should be taken across the private and public sector to increase clarity and promote greater trust.](#)

- Business model: There's an old saying about data being the new oil and that leads to problems with digital identity. Companies want as much information about customers as possible and this is something the internet provides. Many of the new identity schemes – such as self-sovereign identity – would limit the information companies receive. This goes against current business models, even though in event of a breach they would be better off having less information. Companies need to look at a different model when it comes to digital identity that limits the amount of information that benefits the individual.

Recommendation: Further work should be undertaken to develop options for digital identity business models. This work should focus on how the public sector can support increased adoption of credentials that promote individual ownership of data and credentials.

- Inconsistent or incomplete standards: There are numerous identity standards and it's difficult to identify the proper one for various use cases leading to inconsistent adoption.

Recommendation: Enhance interaction between international standards bodies to promote consistent mechanisms for digital identity.



Conclusion

Opportunities exist to mend the fractured global identity ecosystem. As the world takes its first steps out of the COVID-19 pandemic, it is a good time to look at the problems with digital identity and create a plan for mending the disparate systems in existence today.

Acknowledgements

This work was developed by members of the World Economic Forum's Global Future Council on Cybersecurity within the Disruptive Technologies work group which was led by Colin Soutar.

Thanks also to Zack Martin and Ryan Galluzzo of Deloitte & Touche LLP.

Endnotes

1. California investigating hundreds of unemployment fraud cases involving prisoners, <https://ktla.com/news/california/california-investigating-hundreds-of-unemployment-fraud-cases-involving-prisoners/>
2. U.S. Department of Labor, Semiannual Report to Congress, Office of Inspector-General, <https://www.oig.dol.gov/public/semiannuals/84.pdf>



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org