MATTR

FINANCIAL SERVICES WHITEPAPER

The Critical Need for Digital Identity and Verifiable Credentials

MATTR

The Critical Need for Digital Identity and Verifiable Credential in Financial Services
Published by MATTR • info@mattr.global • 12 Madden Street, Auckland 1010, New Zealand

The Critical Need for Digital Identity and Verifiable Credentials in Financial Services

Jo Spencer[1], John Phillips[1], Claire Barber[2] and Luke McIntyre[2]

1 460degrees, L8, 460 Collins Street, Melbourne VIC 3000, Australia

2 MATTR, 12 Madden Street, Auckland 1010, New Zealand
Email: info@mattr.global

Introduction **2**
Executive Summary 2
Paper Context 3
Verifiable Credential Ecosystem 3

The Digital World **4**
Digital Evolution Gets Tough 4
Open Banking – Sounds like a good idea? 4
Complex Relationships and the Identity Challenge 5
Digital Channels First 5
Customer Experience in a Digital World 6
Knowing Your Customer the Right Way 6
Payments – Quicker, richer, better 7
Identity Services 8
Decentralised Identity 8

This paper may be cited as:

MATTR, 2020. The Critical Need for Digital Identity and Verifiable Credentials in Financial Services. Auckland, New Zealand: MATTR. 8 pp.

Introduction

Executive Summary

Perhaps more than any organisation, providers of financial services know how expensive, hard and essential it is to operate in the digital world. Security, fraud, cost and risk are ever present challenges, and made more complex with real-time expectations, more digital offerings and different customer channel options. A fundamental cause of a lot of these challenges is the inability to rely on customer and business identities and the information customers provide to authenticate interactions with the provider.

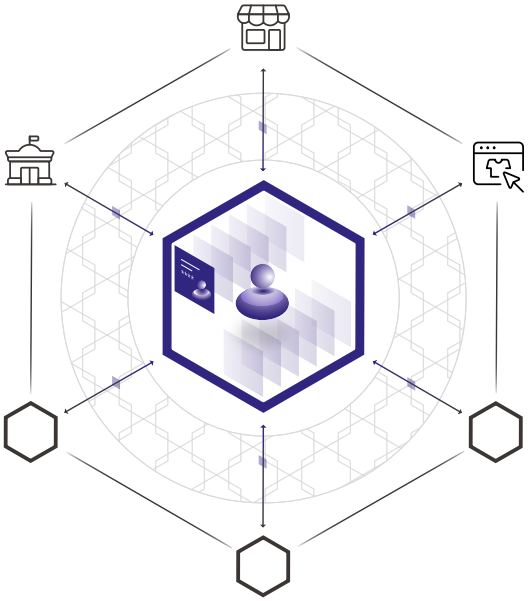
Traditionally, digital identities for organisations and people have relied on creating synthetic customer profiles, specific shared secrets (usernames and passwords), poor-quality or at best sub-optimal verification processes of physical and digital credentials and complex authentication mechanisms that force the customer to behave differently as each provider demands. As a customer, having to do this specifically for so many different digital service providers, makes our digital life a nightmare.

The industry could take a large chunk of cost and risk out of their digital ecosystem and back-office overheads if they were able to identify customers better, confirm that they are in control of each interaction, use a secure link to each customer and verify the information provided by customers in real-time. The result would also be a massive change from the current complex and poor customer experience.

Being able to put the customer in control and able to use verified credentials from authoritative sources, such as banks and the government, for any online interaction would be a game-changing customer experience and provide real customer trust in the process and flexibility to alternative service providers.

Solutions for credential issuing and sharing based on the principles of Self Sovereign Identity (SSI) offer the potential to change the way customers identify themselves and provide information about themselves to banks and other financial service providers. SSI offers a collaborative framework that provides fundamental improvements in how a provider looks to understand their customer, the specific context and meaning of the digital interaction, the security and authenticity of the customer interaction and what data about their customers that they actually need to maintain.

This is the first in a series of whitepapers that explores the current challenges in the digital delivery of financial services, focused on Australia and New Zealand. It explores how providers would benefit from decentralised verifiable credential solutions (based on SSI) and how to fundamentally rethink and address the ever-increasing burdens and challenges to their digital ecosystems and in the digital lives of their customers. This series will be grounded in commercial reality by including input from executives currently dealing with these challenges within leading financial service organisations in New Zealand. It's these individuals that we have to thank for their foresight and leadership.



Self Sovereign Identity is a model that supports the issuing and sharing of verifiable credentials, with the individual (known as a 'holder') in control of the digital interaction. With no single controlling central authority, Self Sovereign Identity is considered a 'decentralised' approach to digital interaction. It often uses distributed ledger technology to enable broad adoption and standardisation.

The SSI model of sharing verifiable credentials in effect **puts the individual in control whilst presenting their identity and data about themselves, digitally.**

Paper Context

This is the first whitepaper in a series, looking at the digital ecosystem in financial services in New Zealand and proposing a fundamentally different way of interacting with customers, managing their information and a liberating model of allowing credentials offered to customers to be used by them as needed. It provides an overview of the current challenges to our financial services providers and identifies radically different approaches to tackling these challenges. Each of the challenges identified will be explored in more detail in their own subsequent whitepapers.

The basis for our insights is the adoption of solutions based on a world-leading decentralised identity model that enables organisations to securely issue credentials to customers and organisations, request proof of credentials from customers and organisations, and verify the authenticity of those proof responses, all with a model that embeds the best privacy principles as a core, foundational element.

Terminology can be a real challenge in itself. 'Digital identity' can mean many different things depending on the audience and context. In these whitepapers, digital identity is a concept of identifying parties using digital channels, leveraging credentials relevant to the context of the digital interaction. This is not only applicable to the 'identification' of organisations and people, but it can consider specific roles and personas (such as the rugby club secretary) and 'things' that need to be identified and can be owned (such as your car or fridge).

Verifiable Credential Ecosystem

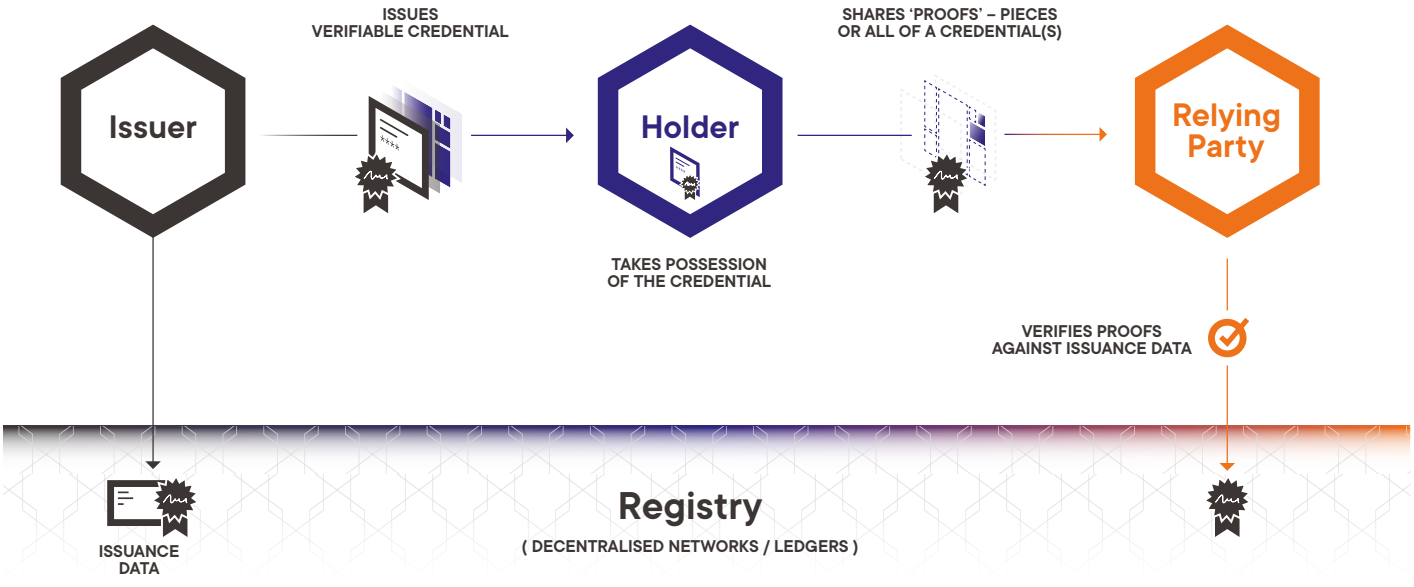
A verifiable credential ecosystem in the Self Soveriegn Identity model involes an 'Issuer', 'Holder' and a 'Relying Party'.

STEP ONE
An Issuer first creates an 'Issuer Decentralised Identifier' on the Ledger. An issuer then uses these to create a credential.

STEP TWO
A new credential is created and signed by the issuer. This is a Verifiable Credential. The Verifiable Credential is then issued to the Holder.

STEP THREE
The Holder uses these credentials selectively in identifying themselves or sharing specific information with a Verifier.

STEP FOUR
Verifiers can check the authenticity of any given credential on the Ledger by checking the issuers signature and the status of the credential on the Ledger.



The Digital World

Digital Evolution Gets Tough

There's no doubt that financial service providers have embraced the digital age over the last 40 years. Internet-based, customer channel interactions are now more critical than the traditional face-to-face, branch-based or phone-based ones. For example, there's quite rightly a major public outcry when the card payment point of sale process breaks down, such is the real-life reliance on this infrastructure.

More recently, digital interactions and channels include mobile apps, online banking, payments at merchants and online, and now with the initiation of payments from other sources (planned with Open Banking and other initiatives) from our traditional banks, 'neobanks' and new providers such as payment mechanisms. The options for interacting with providers of financial services are just exploding with new 'in-app' solutions, payment options, information aggregation, digital on-boarding and comparison services looking to make it better and easier for customers (really?).

Each of the growing number of providers is mandated to verify a customer and each looks to make this as simple as possible, so as not to restrict their own adoption. However, for customers, the combination of all these options makes a massive burden of managing each of these relationships and the information that is required for each. The promise from all is that interacting digitally makes it easier, without the need to talk to anyone – until things go wrong...

We need a step-change in how customers manage their trust in provider relationships, transparent and customer-centred authentication mechanisms, customer enabled control and better standard approaches to the verification of customer credentials. A common, but extensible platform built to support multiple, non-competing initiatives like the Sovrin Foundation[1] will undoubtedly be game-changing.

Open Banking – Sounds like a good idea?

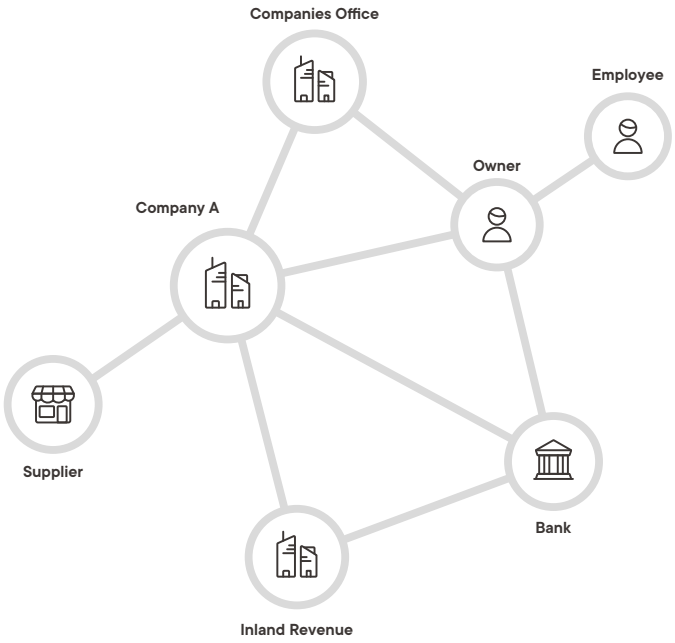
Regulators across the world have looked to improve customers' choice, create the potential for customers to migrate between providers and allow evolution of a controlled and broader environment for information sharing and payment initiation. Whilst the intention of Open Banking and Open Data initiatives is to drive improved products and services from different providers to the customer's benefit, the implementation appears to have unexpected and complex consequences. The critical learning from these initiatives is that without a simplified digital identity and verifiable credentials ecosystem, it's impossible to develop a secure information exchange environment which puts the control into the customer's hands, is easy to use and can evolve to be really useful.

1 https://sovrin.org/

Complex Relationships and the Identity Challenge

Our physical worlds are complex. We have complex and changing relationships, working scenarios, housing and commercial arrangements that are becoming more and more digital in nature. Trying to reflect these relationships and keep them up to date in the context of how we deal with financial services providers is time-consuming and can be very frustrating.

Often, the provider needs to know and verify quite intimate details to be able to offer loans and other new products, provide services or change the relationship with them due to changes in a customer's situation. This makes it hard to comply with regulations and provide good customer service. Any digital identity solution supporting existing and new relationships needs to be able to cater for these complex and changing relationships, including the concept of guardianship and delegate authorities. Decentralised identity solutions are doing just that.



Digital Channels First

Do you remember the first Automated Teller Machine (ATM)? We (who are old enough to remember 1969 in Australia and the early 80s in New Zealand) thought it was brilliant that you could get cash without using a bank book and talking to a branch teller. Whilst it was the first 'digital' channel, it was limited and initially an awful customer experience. Now, in the truly digital age, we have real-time contactless merchant solutions, bank sites and apps, payment wallets on phones and in 'wearables' and, with open banking, we will be initiating transactions and offering products through trusted 'third-parties'. Interestingly, with the reduced dependence on cash, it's the ATM that is not seen as a critical channel in the future.

Whilst the customer channel options are many and growing, the basic challenges still exist. Are you the customer or the account/card owner? Is the transaction secure? Can you do what you're asking to? Is the information you've provided or been given correct and untampered? Has the solution been compromised? Trust in the customer interaction and the digital channel solutions is critical for both the provider and the customer.

With the multitude of interaction options and services provided by each of the many providers out there, consistent changes and evolution is becoming more and more expensive and difficult to coordinate across the industry. Collaboration, coordinated by industry and government bodies, is essential to focus on consistent standards and technology that make it simpler, cheaper and safer to interact in the digital ecosystem.

Customer Experience in a Digital World

Understandably, providers of financial services are looking to differentiate themselves based on customer experience. Each spends a large amount of effort in the design of their digital and physical channels looking for the 'killer experience' or 'killer app'. Often, the focus is how their own products and customer information are presented, rather than the overall customer experience.

Of course, with the increase in provider options and the different digital channel options, our digital world is becoming more and more complex. Even 'digital-natives' struggle to stay on top of how we have to authenticate ourselves to each service provider and keeping the information about us up to date. A digital wallet which provides verifiable credentials, issued specifically to us, combined with sensible use of local biometric verification, provides the promise of a simplifying digital landscape, improved trust and a better experience for us all.

Knowing Your Customer the Right Way

KYC is a three-letter acronym that's becoming widely recognised by the general public. Know Your Customer compliance requirements are imposed through national regulators on the financial services providers (AUSTRAC[1] in Australia and DIA[2] in New Zealand) and they stipulate the expectations on how a customer is verified using Personally Identifying Information (PII) shared either physically using documents or digitally using online services. KYC checks have to be completed before a customer can be on-boarded and allowed to transact and they can present a real barrier to on-boarding customers digitally. The quality of the KYC process depends on the authenticity of the provided information. More often than not, 'verified' copies of original credentials like birth certificates, passports and utility bills are depended on to provide what's known as the 100-point check. So physical verification is open to considerable risk. Digital verification by issuers like the government provide a better quality validation, but the lack of privacy to the customer (as the government is then aware of the customer's activities) is a concern. The reason KYC and it's cousin AML (Anti-Money Laundering) are so well known is because these regulations have teeth and financial service providers are penalised when found not to be doing the right thing. KYC is thought to cost over $150 per customer and over $450m per year as an industry in Australia alone.[3] Yet KYC itself could be done better. Fines for poor KYC, AML, sanctions, breaches and regulatory reporting run into the billions where breaches occur, businesses risk their operating licences and senior executives risk their careers in these cases. So the business case for initiatives covering compliance topics is always easy to justify.

The customer friction in presenting physical documents and providing these to organisations, that may not look after (or destroy) the copies that they take, is significant. This is especially the case where you have to prove a relationship or responsibility (such as a company officer). The suggestion is often that KYC results should be able to be 'reused', rather than done again. The challenge with this approach is that the financial and criminal liability is rarely retained by the original verifier. A bank that knows that the customer has been through another bank's KYC, because the customer has already been given a bank account, will rarely trust the other bank's KYC and will look to do it again for itself. Rather than reusing KYC checks, surely the better approach is to make

1 Australian Transaction Reports and Analysis Centre

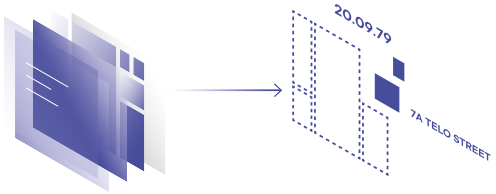
2 Department of Internal Affairs Te Tari Taiwhenua

3 Australian Treasury Department, 2019. Treasury Annual Report 2018-19. Canberra, Australia: The Treasury.

the digital KYC process so easy that it can be done over and over again without creating customer pain or legacy and unprotected data.

With all this personal information floating around, privacy and identity theft becomes a serious concern. Regulators are trying to catch up and the General Data Protection Regulation (GDPR) is starting to have a significant impact on digital data thinking. The most common realisation is that the best thing to do about PII is not to have it at all! This was similar in the payments space with the data regulations (called PCI-DSS[4]) covering the security and management of card information. Card information became 'toxic' and had to be removed, tokenised or encrypted in a very expensive process for all concerned.

So an alternative approach to traditional models of KYC is to allow the customer to hold issued and verifiable credentials, sharing only what's necessary (and that might be the fact that they have them) with the service provider and allowing them to be tokenised and encrypted, such that they are only visible to the parties involved in the sharing process. Again, decentralised digital identity technologies provide the framework, standards and protocols that caters specifically to the issuing, holding and sharing of credentials with greater continued verification, without creating unnecessary customer friction and concern. The customer then retains visibility and control of the sharing process and can always remember what was shared with whom.



Payments – Quicker, richer, better

In the world of the 'always-on' digital economy, expectations of the domestic and international payment mechanisms are becoming untenable, as digital transaction complexity, volumes, compliance requirements and payment options increase. The demand is for real-time, immediate transfer of funds and the associated data, 24/7, with massive pressure to reduce failure rates to nearly zero percent and costs to near zero too. The challenge is therefore to know enough about the parties involved and their account details before initiation, such that payments can be authorised in sync with the broader digital and physical transaction. In this way, payments would become less fragile and more certain between trusted and approved parties. So, the result is fewer failures, the option of simplified point-to-point payment mechanisms and reduced payment costs.

Card-enabled payments have been able to provide basic but broad-reaching payment services for 50 years, and the card schemes and the parties involved have managed the inherent weaknesses (fraud) and inefficiencies over that time. More recently additional ('stronger') verification mechanisms are being regulated to reduce the significant fraud levels and these run the risk of increasing customer friction and creating poor experience.

Domestic and international account-to-account payments are now becoming more real-time. This leads to need for verification of the parties involved, their account details and their ability to transact (from sanctions, Countering Financing of Terrorism (CFT) and AML perspectives) in real time as part of the payment process. Preferably, not after the payment has been completed. The focus from the industry is therefore on pre-validation and compliance.

There's no doubt, an efficient and risk-based digital identity framework would increase certainty and efficiency of payments processing and help to address fraud and black-economy activity.

4 Payment Card Industry Data Security Standard

Identity Services

A NEW PRODUCT SET AND GREATER RESPONSIBILITY?

So, banks and other financial service providers are trusted! Well, that's been the traditional view. But we only currently trust them to look after our money, investments and loans (and there are lots of regulations in place to safeguard this) because there aren't any other real options, other than hoarding cash under the mattress.

The proposal by some is that we get banks and other trusted institutions to provide all the identity services that we need. A model of this is the BankID in the Nordic countries. Even if that made commercial, security and practical sense, which we propose it doesn't, the assumption would be that each organisation providing centralised identity services would be interested in providing wide-ranging capabilities – maintaining your personal information (that is very difficult for them to do) and provide all your requirements irrespective of any commercial implications... and we haven't even started to talk about centralised data breaches and hacking risk, let alone correlation of digital interactions!

We, as customers, want to have the option of using multiple service providers and them ability to migrate to new ones whenever we want to. If we bind ourselves to any one digital identity provider, that may or may not be interested in supporting industry and the broader good, it creates yet another difficulty in spreading out our financial interests or changing service providers.

Any digital identity ecosystem needs to be able to easily extend biologically and commercially and cater to new digital interactions and complex relationships. For financial service providers, they'd be better off issuing specific credentials under their own control and leveraging the primary issuing of personal credentials issued by other trusted entities (such as the government). It just takes a little coordination to make this happen.

Decentralised Identity

THE CORNERSTONE FOR DIGITAL EVOLUTION

All of the topics highlighted in this paper demand a digital identity and verifiable credential capability to build simplicity, authenticity and trust into each of their digital solutions and interactions. No wonder that the focus of technologists and industrial leaders throughout the globe is on the need for standards, frameworks and solutions that provide under-pinning digital identity capabilities.

The beauty of a decentralised digital identity and verifiable credential framework is that the implementation of a broad, non-competitive ecosystem can evolve to provide multiple, joined-up solutions in parallel, driven by different business and customer demands. Technology based on open, global standards can evolve and inter-operate as they mature, because of the design and technical standards on which they are based.

It's critical that risk, regulatory and industry bodies recognise the importance of an interoperable digital identity ecosystem. Once this is agreed and defined, schemes, service providers and technology partners can be coordinated to evolve aligned, practical and commercially sensible solutions that don't build in security weakness, practical complexity and commercial bias. Decentralised digital identity ecosystems and the global standards and governance frameworks provided by these give the best opportunity to make this a reality.

MATTR

The Critical Need for Digital Identity and Verifiable Credential in Financial Services
Published by MATTR • info@mattr.global • 12 Madden Street, Auckland 1010, New Zealand

M20-0205 WS v1

MATTR

www.mattr.global info@mattr.global
12 Madden Street, Auckland 1010, New Zealand