

# The Current and Future State of Digital Wallets

A guide to help understand where the Digital Wallet market is and where it is heading. For business and personal use.

v1.0 2019-04-28

*Author:*

**[Darrell O'Donnell, P.Eng.](#)**

President & CEO

Continuum Loop Inc.



## TABLE OF CONTENTS

<b>1. Executive Summary</b>	<b>6</b>
<b>2. Introduction</b>	<b>8</b>
2.1. Structure of the Report	9
2.2. Report/Project Approach	10
<b>3. What Is A Digital Wallet?</b>	<b>12</b>
3.1. Let's Clear up Some Terms	13
3.2. What Aren't We Covering	14
3.2.1. Payments	14
3.2.2. Personal Data Stores	14
3.2.3. Crypto Wallets	15
3.2.4. Hardware Wallets	15
3.2.5. The Long History of Digital Wallets	15
3.3. What Can't a Wallet Do?	16
3.4. What is an Agent?	16
3.5. The Most Basic Digital Wallet	16
3.6. How Do You Use A Digital Wallet?	17
<b>4. Digital Wallet - Deeper Detail</b>	<b>19</b>
4.1. You Already Have a Digital Wallet	19
4.2. What Is At Risk	20
4.3. Detailed Capabilities of Wallets & Agents	20
4.3.1. Credentials – Receiving, Offering, and Presenting	20
4.3.2. Authenticating – Logging You In	21
4.3.3. Organizing	21
4.3.4. Rendering	22
4.3.5. Personas	22
4.3.6. Private Connections	22
4.3.7. Emergency Access	23
4.3.8. Trust Hubs/Registries	24
4.3.9. Compliance & Monitoring	24
4.3.10. Schemas & Overlays	24
4.3.11. Revocations & Expiries	25
4.3.12. Offline Operations	26
4.3.13. Keys and Secrets	26
4.3.14. Secure Hardware Integration	26
4.3.15. Notification	26

4.3.16. Backup & Recovery	27
4.3.18. Vault Support	28
4.3.19. Multiple Device Support	28
4.3.20. Synchronization	29
4.3.21. Selective Disclosure	30
4.3.22. Manage Guardianship & Delegation	31
4.3.23. Messaging	32
4.3.24. Signing	33
4.4. Guiding Principles for Digital Wallets	33
4.4.1. Consent-Driven	33
4.4.2. Privacy by Design	34
4.4.3. Security by Design	34
4.4.4. Portable and Open by Default	35
4.5. “Stuff” In A Digital Wallet	35
4.5.1. Receipts, Ownership, and Warranties	36
4.5.2. Address Book & Relationships	37
4.5.3. Consent Receipts	37
4.6. Enterprise Wallets	37
4.6.1. Scale	37
4.6.2. Multiple Agents	38
4.6.3. Delegation (Rights, Roles, and Permissions)	38
4.6.4. Protection	39
<b>5. Agents – Deeper Detail</b>	<b>40</b>
5.1. Types of Agents	40
5.2. Who Is In Your Wallet?	41
5.2.1. Emergencies – Break Glass In Case of Emergency	42
5.2.2. Insurers	42
5.2.3. Monitor / Auditor	43
<b>6. State of Tech / Art of The Possible</b>	<b>44</b>
6.1. Current Successes	44
6.2. Where Are Things Working (and Failing) Now?	44
6.3. Where Is It Really Hard?	45
6.4. Further Research and Effort	46
6.4.1. Trust Hubs	46
6.4.2. Credential Lifecycle	49
6.4.3. Certification	50
6.4.3.1. Can We Trust Bubba’s Wallet?	50
6.4.3.2. Certifying Bubba’s Wallet	50

6.4.4. Rendering	51
6.4.5. No Device/No Smartphone	52
6.4.6. Guardianship & Delegation	53
6.4.7. Schemas & Overlays	54
6.4.8. 2FA/UFA Use Cases	55
6.4.9. Backup & Recovery	56
6.4.10. Vault-as-a-Service	56
6.4.11. Break Glass In Case of Emergency	57
6.4.12. Bare Minimum Portability	58
6.5. Standards	59
6.5.1. Protocol Evolution	59
6.5.1.1. Is It Worth The Effort?	59
6.5.1.2. A Small Example – Sovrin Agent-to-Agent	60
6.5.2. Overview of Standards Landscape	61
6.5.3. Assurance Levels	62
6.5.3.1. Identity Assurance Levels	63
6.5.3.2. Credential Assurance Levels	64
6.5.4. PCTF	65
6.5.5. Portability	67
6.6. The User Experience Challenge	67
6.6.1. Organizing and Finding My Stuff	68
6.6.2. Invites, Offers, and Requests	68
6.6.3. What’s Normal (What’s Weird)?	69
<b>7. Business &amp; Markets</b>	<b>70</b>
7.1. The Evolution of Digital Wallets	70
7.1.1. Stage 1 – Basic Digital Wallets	70
7.1.2. Stage 2 – Specialized Applications and Digital Wallet Platforms	70
7.1.3. Stage 3 – Broad Platform and Operating System Integration	71
7.2. Early Business Approaches	72
7.2.1. Single-Purpose Use Cases	72
7.2.2. Backup & Recovery is Mandatory	73
7.2.3. Simple Trust Hubs	74
7.3. Influence Things	74
7.4. Help Build the Ecosystem	76
<b>8. The Upcoming Wallet Wars</b>	<b>78</b>
8.1. I Want To Build My Own	78
8.2. Surviving – Push the Standards	79
8.3. Acknowledgements	80

## Disclaimer and Author's Remarks

This work is published by Continuum Loop Inc. (Continuum Loop) and reflects the corporate viewpoint of Continuum Loop and its leadership. Individuals and companies that participated in this study may have their own views and though mentioned, may not support the views espoused in this report.

Continuum Loop has released the PDF version of this report under a Creative Commons ([CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)) licence. The hope is that the content here will help begin discussions and spawn new artifacts and thinking.

On a personal note, I'd like to state that I don't normally "do reports". I tend to be deep into execution or intervening in teams that need to get to delivery. The Digital Wallet space was so vague and uncertain that several leaders looked around and realized that if someone didn't start digging we wouldn't have a baseline. The leaders who pushed me to dive in are incredible and their sponsorship of the work made a huge difference. Big thanks go to Mike Brown of ATB Financial, Andrew Johnston of Telus, and John Spicer of 2Keys for their ongoing support.

I know that the content may feel wrong and I am OK with that. Our community needs to get clear quickly about what a Digital Wallet is and what it means to create and use them. If this report helps, I have accomplished my mission.

Reach out for a discussion.

I look forward to hearing from you.

Cheers,

Darrell

Darrell O'Donnell, P.Eng.  
President & CEO  
*Continuum Loop Inc.*

Twitter: [@darrello](https://twitter.com/darrello)

# 1. Executive Summary

The World Economic Forum states that we are in the beginning of the Fourth Industrial Revolution<sup>1</sup>. Technologies are converging and provide immense potential for shifting how we can improve every aspect of our lives.

Underneath all of that technology lies the internet, which has a flaw that could have been fatal – until recently it has lacked a built-in digital identity. Hacks to get around this missing piece have resulted in huge security gaps and abusive digital relationships. The availability of a Digital Identity that makes personal and business sense is removing this shortfall and multi-billion dollar industries will be impacted<sup>2</sup>.

Organizations and people who understand how digital identity works will see the early benefits and likely receive more of the benefits. The stakes are enormous:

*“digital ID has the potential to unlock economic value equivalent to 3 to 13 percent of GDP in 2030”<sup>3</sup>*

– McKinsey Global Institute

The sponsors of this study recognize that a Digital Wallet is a requirement for us to be able to assert the appropriate control of our Digital Identities. Without a Digital Wallet, which allows us to control our Digital Identities – both at a personal and business level – we won’t be able to realize the benefits.

The study culminates with this open report. This report provides:

- definition of what a Digital Wallet is
- clarification about where the Digital Wallet industry and ecosystem is currently
- guidance for organizations to move forward as the Digital Wallet ecosystem forms

The Digital Wallet ecosystem is in a very early stage. Organizations that are true innovators will find a rich and frothy environment that they can work in, influence, and drive forward. Those organizations that only use “innovation theatre” should stay away for now and let the market formalize. Be realistic – innovators are a very small percentage (2.5%<sup>4</sup>) of society.

---

<sup>1</sup> [The Fourth Industrial Revolution - What It Means and How to Respond](#), World Economic Forum

<sup>2</sup> [Our Shared Digital Future](#) - World Economic Forum

<sup>3</sup> [The value of digital ID for the global economy and society](#) - McKinsey Global Institute

<sup>4</sup> [Diffusion of Innovations](#) - Wikipedia

Simple use cases are finding success and the learning is accelerating. Small projects are gaining traction. The Digital Wallet ecosystem is shifting rapidly and leaders are emerging. Understanding where you and your organization fit is crucial.

This report aims to be a starting point. The Digital Wallet space is immature and many predictions here will be wrong – either in timing or even in intent. However, the shift to a world where we have a Digital Wallet that empowers us is happening. We aim to provide the basics so you and your organization can begin to plan, explore, and learn.

## 2. Introduction

The world of Digital Identity is changing. People and Organizations are beginning to assert control over their digital lives. Centralized services still dominate but the advent of self-sovereign identity and verifiable credentials have changed the landscape.

Our ability to control what information we share is increasing – from identity documentation to various forms and data that others need. We can accomplish much more in this new and rapidly evolving world.

The experts are creating the underlying technologies from blockchain/distributed ledgers through distributed key management. These are the building blocks that nobody will see in the near future.

Governments are issuing Digital Identity Documents including digital driver’s licences. Organizations are issuing various credentials for employment, education, and more. We’re seeing digital ownership become more common.

We’re told that our Digital Wallet is where we put these things to keep them safe and use them.

But what is a Digital Wallet? Ask a dozen people and you’ll get a dozen different definitions.

As leaders in Canada and abroad met at the Internet Identity Workshop #25<sup>5</sup> the ideas behind “what a digital wallet is” began to form. Global leaders in the identity space had early ideas about what the advent of Verifiable Credentials would mean to People and Organizations.

<i>definition</i>	<b>Verifiable Credential</b>	<i>A Credential is a set of one or more claims made by an issuer. A <b>Verifiable Credential</b> is a tamper-evident Credential that has authorship that can be cryptographically verified.</i>
	<i>W3C Verifiable Claims Working Group<sup>6</sup></i>	

<sup>5</sup> “IIW 25 Session Notes - IIW.” Accessed February 16, 2019. [https://iiw.idcommons.net/IIW\\_25\\_Session\\_Notes](https://iiw.idcommons.net/IIW_25_Session_Notes).

<sup>6</sup> <https://www.w3.org/2017/vc/WG/>

It is clear that Digital Wallets form the basis of how we issue, store, share, and verify these verifiable credentials. Without a Digital Wallet we can't really use the verifiable credentials effectively, nor do many other things in our digital lives.

Digital Wallets are clearly critical to the evolving digital landscape. They are poorly understood, though.

The simple fact is that as an industry, we do not know what a Digital Wallet is or what a Digital Wallet needs to become.

In order for Organizations to plan for their digital future a deep understanding was needed, of what a Digital Wallet really is. A study was commissioned and this report is one of the outputs of that study.

This report aims to lay down a baseline understanding of what a Digital Wallet is. This definition will not survive for long. The study sponsors went into this study knowing that the landscape is changing. This report serves as one of many pieces that will hopefully help define where we all need to go.

The report is structured to lay down what a Digital Wallet is and what it can do, then discuss where things currently stand. Finally we provide guidance on approaches that organizations and businesses can take.

Our current understanding of what a Digital Wallet is will evolve quickly. In time this report will be revised or replaced.

## 2.1. Structure of the Report

This report is set up to provide two main things:

- Technical – explanation of the various functionalities and capabilities of Digital Wallets - that either exist now or will need to be built in order to realize the Digital Wallet ecosystem.
- Business – advice on approaches to build out a Digital Wallet system - there are many capabilities required but building them in a particular order will allow the ecosystem to grow faster than it would without considering the bigger picture.

The technical sections are intended to provide a few levels of detail:

- What is A Digital Wallet – we go through a high level view of what Digital Wallets are, covering the major capabilities and pieces.
- Digital Wallet Deeper Detail – we cover, in depth, many of the capabilities that are crucial for Digital Wallets.

- Agents Deeper Detail – Agents are unique enough that we go into depth about many different kinds of Agents. Entire businesses and likely industries will form around these Agents.

The business sections discuss where things are (hint: it is VERY early in the creation of a new ecosystem), where we need to go, and a recommended path to get there:

- State of Technology – we will describe what the current state of affairs is as far as the capabilities that are needed for basic and advanced Wallets.
- Art of the Possible – leans into looking at what a Digital Wallet enables - and where the bleeding edge of research and thinking is headed.
- Business & Markets – describes where organizations can focus efforts to explore and build capabilities.
- The Upcoming Wallet Wars – in this short section we'll introduce the idea that the Digital Wallet space is going to see activity that is similar to the early browser wars where vendors and consortia battle things out to win your business and use.

## 2.2. Report/Project Approach

In fall 2018 a group of Canadian companies banded together to commission a focused effort which would produce a report for the global community that gathered various thoughts, ideas, and approaches which would address the evolving needs of a Digital Wallet. These project sponsors recognized early that a “Wallet” was not a small project and that no single organization could create a full Wallet. Even the largest organizations don't have the resources to create a full Digital Wallet. Nor do they have the mandate to control something that is becoming so important for society.

The market requirements for Digital Wallets were researched and determined to be quite broad. The project team engaged in the research report realized that the broad discussions about Digital Wallets needed more depth and more breadth as many communities use the term “wallet” and “Digital Wallet” quite differently. The project sponsors recognized that the community needed a beginning point for discussion.

Through internet research that identified over 250 blockchain/crypto/wallet projects the beginning of a simple delineation formed. The “crypto” space is well served at the moment with Cryptocurrency Wallet applications that meet the needs of the “crypto” community – as obscure as those tools are. As an example, the following 19 logos were gathered under a quick “get me wallet logos that work on a white background in less than half an hour” – providing proof that the Crypto Wallet space is truly enormous.



The line between a Crypto Wallet and a Digital Wallet began to form. This report focuses on the non-crypto aspects of a Wallet (see [3.2. What Aren't We Covering](#)).

Following the internet research engagement a large number of thought leaders were contacted to discuss what their ideas were about Digital Wallets. Whitepapers, blogs, podcasts, Twitterati, and more were engaged. Discussions on the open internet and in private ensued. Additionally work was undertaken at Rebooting Web of Trust 7 (Toronto, Ontario 26-28 September 2018<sup>7</sup>) and presentations at the Internet Identity Workshop (Mountain View, California 23-25 October 2018<sup>8</sup>).

In December 2018 the project sponsors met to create another delineation - between what content would be private and public. The overall decision was that the vast majority of information would be publicly released. The strategies and tactics that applied to the project sponsors will remain private.

---

<sup>7</sup> RWoT7 in Toronto, Canada (September 2018). <https://github.com/WebOfTrustInfo/rwot7-toronto>.

<sup>8</sup> "IIW 27 Session Notes - IIW." Accessed February 16, 2019. [https://iiw.idcommons.net/IIW\\_27\\_Session\\_Notes](https://iiw.idcommons.net/IIW_27_Session_Notes).

### 3. What Is A Digital Wallet?

The general idea of a Digital Wallet is pretty simple – it’s a Thing that we put our Stuff in<sup>9</sup>. The hard part comes when we have to identify what is that “Thing”, what “Stuff” do we put into it, and even, what does it mean to put “Stuff” in it? What about getting our “Stuff” out? Updating our “Stuff”?

The real-world parallel of a wallet is only so helpful. We all have totally different ideas of what goes into our wallets. Some people put just a bit of cash, a credit card, and likely a driver’s licence. Others have numerous currencies, many credit cards, loyalty cards, multiple identity documents, receipts, photos, tickets, and more.

But we call it all a wallet.

The same is true about Digital Wallets. They have a huge range of capabilities. Crypto Wallets typically store only the keys and addresses of wallets that live in the blockchains underlying each cryptocurrency. Other digital wallets (e.g. Pillar<sup>10</sup>, Connect.Me<sup>11</sup>, [Digi.me](https://digi.me/)<sup>12</sup>, Minerva<sup>13</sup>) are focused on very specific areas of the broad Digital Wallet space.

The Digital Wallet space is broad – and the purpose of this report is multifold:

- Explain the overall capabilities that define a Digital Wallet – both on a Personal and Enterprise basis (yes, they are different).
- State an opinion of where each of the capabilities sits – is it real and live in the world yet, or purely aspirational – or somewhere in between?
- Provide some recommendations and plans for approaching the Digital Wallet space. The space is enormous – and the efforts will exceed the resources of all but the world’s largest companies.

First off, we need to lay down some early terms. More terms will be defined throughout the report but these three terms are critical to understand the viewpoint from which this report was created.

As an introductory concept this wallet, Minerva from Lab10 provides the ability to manage multiple personas. You can see on the right image the personas that splits out an individual’s citizen, work, and judo lives.

---

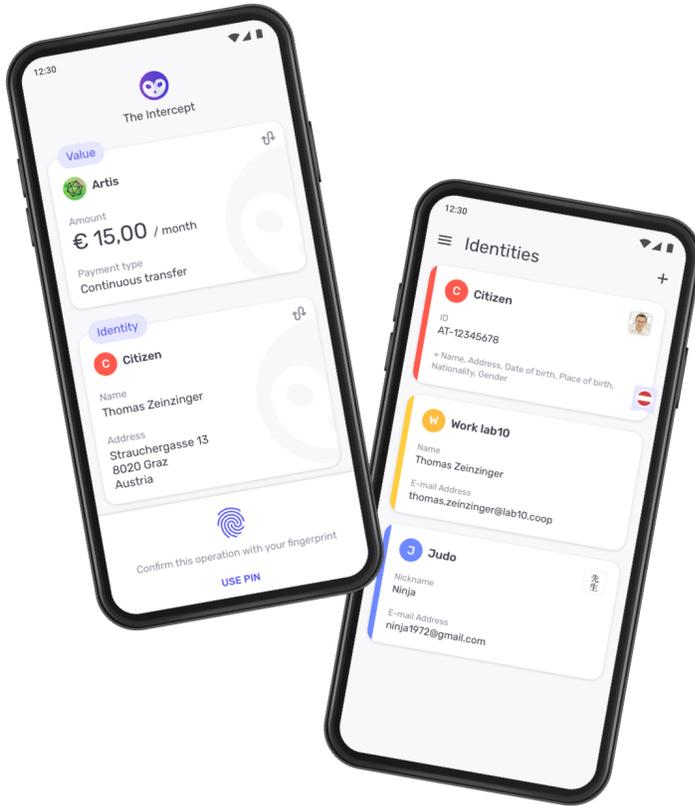
<sup>9</sup> Credit for this “things and stuff” approach goes to John Jordan, who learned it from his community and shared with the report author.

<sup>10</sup> <https://pillarproject.io/>

<sup>11</sup> <https://www.evernym.com/products/>

<sup>12</sup> <https://digi.me/>

<sup>13</sup> <https://lab10.coop/en/projects/minerva>



Source: [Lab10](#)

### 3.1. Let's Clear up Some Terms

The Digital Wallet space is nascent enough that there isn't enough agreement on terms, so you and I are going to need to agree on a few terms to keep things straight. We need to be aware that these terms will likely change over time. At the end of 2018 this is the best that I can do for you.

OK – the key terms that we'll use throughout this report are:

- **Wallet Storage** – the encrypted database of keys, credentials, and other information that is put into a wallet. This is the Thing that holds your Stuff.
- **Agent** – the software service(s) that manage things on your behalf. Agents put Stuff into your wallet, take Stuff out, process Stuff, create Stuff sometimes, and keep you connected

These two building blocks lead us to a Digital Wallet – Wallet Storage and Agent(s) combine to create an application that is going to shake the foundations of the internet and more. It is, in some ways, our digital twin – holding various aspects of our Digital Identity, our relationships, and more.

**WARNING**

*The Sovrin developers use a precise definition of Wallet Storage and call it a Wallet – which is potentially misleading for the non-developer type. “A software module, and optionally an associated hardware module, for securely storing and accessing Private Keys, Link Secrets, other sensitive cryptographic key material, and other Private Data used by an Entity. A Wallet [Wallet Storage] is accessed by an Agent. In Sovrin infrastructure, Wallets [Wallet Storage] implement the emerging DKMS standards for interoperable decentralized cryptographic key management.”*

We’ll get deeper into each of the above but that’s enough to ground the discussion. I am looking forward to better terms arising. For now, the debate about names, and what is what, is holding us back.

## 3.2. What Aren’t We Covering

### 3.2.1. Payments

Payments, whether traditional or crypto, are well handled and exploring them further isn’t warranted in this report. Payment rails are well supported in Canada and around the globe. They follow standards that are set by many parties and don’t really impact our discussion in this report. Adding Identity to existing payment rails is certainly relevant but is out of scope for this document. Over time, Digital Wallets and payment rails will need to connect and support each other but again, that’s out of scope for now.

Though some casual mention of payments and transactions may be made throughout, they are considered generic.

### 3.2.2. Personal Data Stores

<i>definition</i>	<b>Personal Data Store</b>	<i>A personal data store (PDS), vault or data locker is a service to let an individual store, manage and deploy their key personal data in a highly secure and structured way. It lets you keep your own data and also acquire and reuse proofs of claims or of relationships and qualifications (such as bank account, verified address, driving licence or passport).</i>
	<i>MyDex<sup>14</sup></i>	

<sup>14</sup> [“Understanding Personal Data Stores \(PDS\)”](#), Mydex, 01OCT2015 (web archive)

A Digital Wallet is not a Personal Data Store (PDS). We are not here to talk about where we store all of the digital information that we gather over our lives – though the delineation of what a wallet is as opposed to a Personal Data Store is not clean. We may have immense amounts of information in our PDS – movies and music, health and financial records, emails and messages, and much more. The PDS industry is well suited to the bulk management of personal data – but it will have Digital Wallet needs as well.

As we go through this report we will discuss many topics that relate to PDS. We'll keep them in mind but focus on the Digital Wallet aspects.

### 3.2.3. Crypto Wallets

The crypto world has hundreds of Wallet applications that support various different cryptocurrencies. They tend to be either single-currency, supporting only one cryptocurrency, or they can handle multiple currencies. Regardless, they are largely a way to manage the keys that control a Wallet address (or addresses) on a particular blockchain. They handle sending and receiving of transactions. That's largely it.

Many debates exist about the user experience of Crypto Wallets. Engaging in discussion with the crypto maximalists can show a belief that these Wallets are already done – they work for everyone. The simple reality is that Crypto Wallets are incredibly complex (which leads to a poor user experience) and potentially dangerous (the loss of keys; cold storage approaches). The crypto world does not welcome such discussion, however.

One key point about Crypto Wallets is that over time, their obscure usage will likely just end up being something that Digital Wallets “just do”.

### 3.2.4. Hardware Wallets

Related to Crypto Wallets is the early-stage Hardware Wallet Systems that provide “cold storage” for cryptocurrency. At the time of writing there are no Hardware Wallets that provide full Digital Wallet capabilities – they are laser-focused on managing keys for cryptocurrency usage. In time Hardware Wallets may provide self-managed “vault” capabilities but the industry is not close enough to that level to warrant further discussion.

### 3.2.5. The Long History of Digital Wallets

Wallets have a long history – decades in fact – of being “the app to watch”. Twenty years ago Microsoft released Microsoft Passport as an attempt to get information managed in one place: single sign-on and credit cards – all managed for you. It failed, devolving into a federated sign-on capability over the last 20 years. Since then there have been innumerable wallet initiatives that have largely failed – though there are nuggets of innovation that will come to fruition as the Digital Wallet forms.

Largely speaking, the historical wallet approaches have failed for some or all of the following:

- they were closed systems created to serve particular players and they locked in their users
- they were too ambitious – you can't eat the elephant in one bite no matter how big you are

But that's not the point of this report. This report is about what a Digital Wallet is, what is needed to create one, and the business behind those.

### 3.3. What Can't a Wallet Do?

If we take the technical/developer view of a Wallet – or look at our physical wallets – we realize that a Wallet is really just a dumb storage device. Our Wallet can't put anything into itself – nor remove anything. It can't organize things or take a few pieces of information from one credential and pair that up with more information from another. It really is just a Thing to put Stuff into.

So how do we use a Wallet? In the physical world we use our hands, eyes, and brains to utilize the Stuff that we have in this Thing that we call a Wallet.

But in the Digital Wallet world we need software to do this for us – to act on our behalf. We need to control them and ensure that they are acting on our behalf – not somebody else's control unless we are totally OK with the idea of somebody else having that control.

That's where Agents come in.

### 3.4. What is an Agent?

Simply put, an Agent is a piece of software that acts on the behalf of an Identity Owner – a Person, an Organization, or a Thing. It does a few things at minimum to keep you connected and secure:

- it sends and receives messages
- it encrypts and decrypts information to keep your information private
- it signs digital information on your behalf
- it manages information in your Digital Wallet
- hopefully, it backs up our Stuff and allows us to restore

We'll dive deeper into what else Agents can do in [Agents - Deeper Detail](#)

### 3.5. The Most Basic Digital Wallet

In this short section we will discuss the most basic of Agents and Wallet Storage – the guts of a wallet. We will go deeper in the next two major sections of the report.

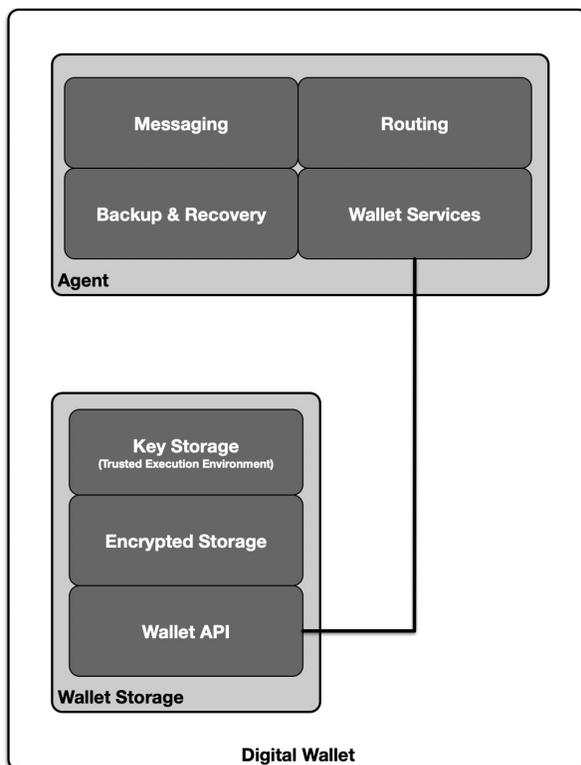
As we mentioned earlier, a Digital Wallet is comprised of an Agent and Wallet Storage. The role of the Agent is at minimum the following:

- It sends and receives messages – to ask for and add credentials at minimum.
- It may communicate with another Agent
- It should provide an ability to back up and restore the contents of a Wallet.

The Wallet must be secure enough to protect the Stuff it contains:

- Keys
- Various items stored in Encrypted Storage – such as Credentials

The following figure shows the basic components of a Digital Wallet.



### 3.6. How Do You Use A Digital Wallet?

Currently you likely have apps on your phone that do portions of what a Digital Wallet will do in the future. We have apps like Apple Wallet and Google Pay that hold payment cards and tickets. We have tools like Google Authenticator that allow us to provide additional authentication security. We have notes in various places with key information. We have photos of key documents - but extremely few authorities recognize the legitimacy of a photo of your driver's licence. We keep our receipts in various places – photos, emails, and in specific apps like Dropbox. We have apps that let us pay using QR codes though they haven't taken off in Canada and the US like they have in Asia (e.g. WeChat Pay).

We have a lot of pieces of a wallet, but they are kind of like using a paperclip to hold cash – they do one thing (maybe) reasonably well, but they don't work together.

We don't have a single application that mimics what our physical wallets do. We don't have apps that automatically know what information is being requested – or what information is required to be presented. We don't have apps that use standards to communicate those requests. We don't know what many apps are doing with our information either so we don't (or shouldn't) trust these apps with our sensitive information.

### **Story:** A Family Trip Today and Tomorrow

When we go on a family trip we gather various information in many places. The author recently went on a trip with three family members. The following information was gathered – in various places:

- hotel reservations – managed in [Booking.com](#) app
- apartment rental – managed in VRBO app
- extra health insurance – paper received from Blue Cross and photos taken as “just in case” measure
- plane tickets from two airlines that wouldn't work together – so electronic tickets couldn't be used. Paper tickets gathered at two different airline counters in two airports
- passports – held in hand at times, and in lockable hardcase at others
- cash – portion held in wallet and portion in a lockable hardcase
- credit cards – held in two wallets (full size and a travel size)
- rental car agreement – in [Avis.com](#) app, though the rental actually occurred using paper and with carbon-paper based payment slip at smaller rental agency

The check-in process at each location was relatively painless as the family was fairly well organized and the bookings were largely at small facilities that had limited business. Still, the interactions were far from seamless. Concluding the rental car work required destroying the carbon that held the credit card information (in case of additional expense), paying cash for missing fuel, all conducted in a sweltering parking lot while the remainder of the family waited elsewhere.

In the Story (we'll have a few of these Stories throughout the report) we note that through the whole engagement there were no real linkages between things, e.g. was the insurance on the rental car, as provided by the credit card sufficient? There was no linkage between the handwritten receipt from the hotel and the combination of cash and PayPal payment used to pay for services. The rental car company had no proof that the driver was capable of handling any excess payments had any been required. The driver's licence that was presented was real but could easily have been a fake.

These gaps create friction in our day-to-day lives. Much of that friction can be reduced in a world where we have Digital Wallets in place. Particularly the linkages – but that raises a major concern: privacy. Let's take the car rental – and consider that this was all in a developing country that doesn't have the same privacy protections as Canada. We don't want a rental car agency in another country knowing everything about us. We don't want them knowing the credit limit on our credit card; nor the exact limits of insurance. They simply need to know that their needs will be met. That includes that they can trust the information that is presented – without needing to know more than required. We need our Digital Wallet to be able to provide information to others without revealing too much. In [4.3.20. Selective Disclosure](#) we discuss how such mechanisms can work.

## 4. Digital Wallet - Deeper Detail

Now that we have discussed what we won't be covering let's get into the meat of our discussion – what does a Digital Wallet do for you, and what will it mean?

### 4.1. You Already Have a Digital Wallet

We're beginning to sense that our Digital Wallet is going to become more important to us than our physical wallets. Think about what you would rather leave at home when you go out – your phone or your physical wallet? Many of us can make it without the wallet – but without our phones we feel naked.

Why is that?

Our phone is already our Digital Wallet. It isn't nearly where Digital Wallets are going to be but it is already doing many of the things that we expect a wallet to do. With our smartphone we can:

- pay for things
- send and receive messages
- receive and show credentials
- manage our keys – though we don't have a clue how or why we need this...

What we don't have is a coherent way of using any of the above. It varies wildly and most of it isn't easy to use.

## 4.2. What Is At Risk

Digital Wallets are already around as we have mentioned but they are in a very early state. As Digital Wallets evolve though there are risks that need to be acknowledged and mitigated. The risks at this early stage are:

- Lock In – with a lack of open standards and much to learn it is quite possible that early Digital Wallets will effectively hold your information hostage as you won't be able to move information around.
- Surveillance – what assurances do you have that the Digital Wallet application that you're using isn't sending information off to an entity that you haven't agreed to share with (e.g. company or state actor)?
- Theft & Loss – Digital Wallets can be stolen physically (i.e. your Smartphone is stolen or lost) or virtually (i.e. your Digital Wallet has been taken over due to key compromise).
- User Experience – in the early days the user experience of using Digital Wallets will be crucial. People will not adopt things if they are confusing or difficult.

## 4.3. Detailed Capabilities of Wallets & Agents

The earliest Digital Wallets hold a limited set of information. Mainstream Digital Wallets like Apple Pay and Google Pay allow simple information to be "carried" inside them:

- credit cards
- tickets (e.g. plane tickets, event tickets)
- Other basic credentials (e.g. loyalty reward virtual card)

Over time more and more types of information will be useful in a Digital Wallet. This section briefly describes some of the capabilities that Digital Wallets are beginning to (or will) support.

### 4.3.1. Credentials – Receiving, Offering, and Presenting

In order to use Credentials our Wallet needs to be able to:

- accept them from others
- request them from others
- respond to requests for them
- and offer them to others

While those capabilities above seem so simple the protocols to do each of them are just being created. Most early stage Wallets have the ability to do some of these tasks but the user

experience is so complicated that only the most dedicated users will ever attempt to perform them.

The [Credential Lifecycle](#) needs to be supported as well, where Credentials may be revoked, updated, and expire.

### 4.3.2. Authenticating – Logging You In

One of the more exciting uses of Digital Wallets is that they allow us to log in to websites and other services with far higher security. They can also make logging in much simpler too. There are two early use cases that are actively being used in various industries including banking:

- **Second-Factor Authentication (2FA)** – 2FA is typically used in combination with traditional username and password. Either as part of logging in or for high-value transactions a Digital Wallet can be used to provide 2FA capability. This increases the security and relative ease of use as most 2FA solutions require dedicated devices or software that may be difficult to use.
- **Passwordless Login** – Multiple initiatives are underway to remove the need to use a username and password. Because our Digital Wallet provides multiple factors that fit authentication (something you have, something you know, and something you are) the credentials and connections that it manages can provide better security and replace username and password use. There are multiple standards that apply. We'll discuss them in Section [6.4.8. 2FA/UFA Use Cases](#).

Our Digital Wallets can help us transition to a much simpler and more secure way of accessing the systems that we use daily.

### 4.3.3. Organizing

Managing many (hundreds or thousands) of credentials mean that a Digital Wallet must be able to organize information to allow its owner to find the information they need. Organizing the stuff in a Digital Wallet is going to be one of the key challenges for the foreseeable future – we just don't have user experience paradigms that work with the amount of Stuff we can keep in a Digital Wallet.

Being able to find information in your Wallet is crucial. However, knowing what information may be used to satisfy a request makes it easier. Imagine a police officer asking for your driver's licence – that's a pretty simple request and easy to respond to (hand your driver's licence over). What about someone requesting an address from you? Depending on the level of assurance required you may present a phone bill, a library card, or just a piece of text that you typed in yourself. Managing the pieces of information is getting hard at this point.

Once we start to look at the other "Stuff" in our wallet we quickly get to the point where hundreds or thousands of items need to be managed. That is simply beyond the capacity of

most folks. Our Digital Wallet needs to help us here. Our Digital Wallet and the Agents that are contained in it have more context – about what we are doing, what is required, what options we have, and more. Agents and the user experiences that evolve over the next few years will be helpful in managing the increasing amounts of information that we hold.

### 4.3.4. Rendering

The current leading solution for specifying digital credentials is the W3C Verifiable Credentials specification<sup>15</sup>, though the specification is still in early days and not a full-fledged standard. It allows for rich data to be shared but there is no direct consideration of how the data will be shared visually. The technical details behind sharing a credential digitally is understood – but what a credential looks like to a human isn't. We don't have any norms about what a digital credential should look like. Some want a digital driver's licence to look just like a physical one – but others feel vehemently that is inappropriate.

For text data the only consistent approach is to use the key names (e.g. "date\_of\_birth") and the value associated (e.g. "1970/12/31") – which leads to a very poor user experience.

For non-text data, such as images, there are no clear guidelines about how a credential should look when viewed.

Standards and best practices will evolve, likely based on a subset of HTML and CSS for simplicity and security.

### 4.3.5. Personas

When we look at our lives we realize that we aren't a single "person". We are different depending on who we are dealing with and what we are doing. We may have multiple different relations with a particular person – a close friendship and a business partnership for example. Yet most systems see us as a singular being.

Digital Wallets will need to support the concept of Personas – allowing us to represent ourselves as needed. The need that drives how we present ourselves may be personally driven (e.g. I decide what to share with you) or mandated (e.g. border control has a very limited set of credentials that it will accept). Regardless, we need to be able to support the multiple personas that we use on a day to day basis.

### 4.3.6. Private Connections

A Digital Wallet maintains connections to various other entities: People, Organizations, and Things. These connections need to remain private so the owner of the Digital Wallet can maximize both privacy and security. To that end a Digital Wallet should use unique, pairwise

---

<sup>15</sup> <https://w3c.github.io/vc-data-model/>

unique identifiers for each and every connection that it establishes. These pairwise DIDs allow each relationship/connection to be controlled independently (e.g., keys rotated, DID terminated/burned). The benefits of pairwise DIDs<sup>16</sup> amongst many others, include reducing correlation risk and allowing for key rotation without impacting other relationships.

<i>definition</i>	<b>Decentralized Identifier (DID)</b>	<i>A new type of identifier developed for decentralized systems as defined by the <a href="#">W3C DID specification</a>. DIDs enable interoperable decentralized Self-Sovereign Identity management. A DID is associated with exactly one DID document. The Sovrin Technical Governance Board defines the technical specifications for a Sovrin DID in the Sovrin DID Method Specification.</i>
	<i>Source: Sovrin Glossary</i>	

#### 4.3.7. Emergency Access

A Digital Wallet will hold crucial information that may be useful in the event of an emergency. Various types of information can be compartmentalized and made accessible through various methods under various conditions such as:

- medical emergency – first responders and medical personnel/institutions will need access
- death or incapacitation – would potentially require legal intervention and consideration of legal authority

We see early Wallets like Apple Wallet allowing for an emergency mode. Your author provides information about a peanut allergy that anyone can use if they have access to his phone. The information is very limited and there is no restriction to who can access the device. However, if a bona fide first responder could prove that they are a first responder (e.g. if they had a First Responder credential that our Digital Wallet could query and confirm), we may release far more information.

So our Digital Wallet needs to consider what information can be provided and under what conditions it will allow release. There are many areas that need to be explored. See section

<sup>16</sup> See <https://forum.sovrin.org/t/the-benefit-of-pairwise-dids/628/3>

[6.4.11. Break Glass In Case of Emergency](#) for an idea of the research and development that is needed.

#### 4.3.8. Trust Hubs/Registries

In order to “trust” the various Credentials that end up in a Wallet we need to be able to know that the Issuer of the Credential is trusted in the first place. Every Credential is created by an Issuer – so knowing how that Issuer’s authority is established is crucial. Digital Wallets will use and maintain Trust Hubs and Trust Registries to know which Issuers should be considered “trusted”.

We need to know that our Digital Wallets are using the right sources of truth, especially in an increasingly decentralized world. As time goes on there will be definitive sources (e.g. a Trust Hub that lists all government Issuers for a country) but initially the opportunity for spoofing and fraud needs to be considered. An enterprising young person may easily create a series of fake Digital Identity Documents masquerading as a province that hasn’t yet started doing so.

Further detail can be found in Section [6.4.1. Trust Hubs](#).

#### 4.3.9. Compliance & Monitoring

Depending on the needs of a Digital Wallet owner there may be a need to invite Agents that perform monitoring and compliance of particular activities in a Wallet (e.g. a bank may require that an enterprise attach an audit agent that relays information about particular activities).

We therefore need to establish whether we bring a monitoring Agent into our Digital Wallet voluntarily or under mandate. Consider the following examples:

- **Health Receipt Monitor** – imagine a software agent that makes sure all of your health receipts go into a list that you can easily share with your health insurance provider.
- **Company Credential Usage Monitor** – imagine your company requiring an Agent that monitors and logs any of the authentication or signing activities that you are doing with the company-issued Credentials.

#### 4.3.10. Schemas & Overlays

Digital Wallets will be sharing and using Credentials of all types. Like any other data-centric system (yes, a Digital Wallet is a system) we will need to get some kind of standardization about how certain things look at the data level. Credentials like driver’s licences, passports, and even receipts can use well-known Schemas. When a Credential uses a well-known Schema our Digital Wallet can do things for us that make our lives much easier.

For example, using well-known Schema (more in [R&D Schemas and Overlays](#)) will help us exchange key information – including contacts, receipts (with the ownership that we discussed earlier), and more.

Additionally, by using well-known Schema we can also use a technology called Overlays to ease how we do things. Overlays allow us to protect private information, view things in standard ways, and more.

A simple example of the use of an overlay is shown below. United Airlines tickets in Apple Wallet adds a graphic marker (yellow “hand drawn” circle) to indicate a change that has occurred to a Credential – in this case, a gate change. This visual indication that United Airlines pushes to a wallet helps understand what information changed.

### STORY: Overlays Example – Driver’s Licence

As an example, imagine you are pulled over by a police officer and the officer requests your driver’s licence and registration. It would be normal for the police officer to require the full details from your driver’s licence. Using that same Credential at a bar to prove your age of majority would be a normal thing to do as well – but they don’t need the same level of information. The bar needs to know that you are old enough to drink but they don’t need the intimate details that are in your driver’s licence Credential.

An Overlay can support the above case. Your Digital Wallet would handle most of this for you. When asked by a police officer for your driver’s licence they would also provide the law-enforcement Overlay that they require. Similarly a bar could ask for the credential with an age-of-majority Overlay and your Wallet would handle that. Your Wallet can also protect you from privacy violations – for example, if the bar asked for your driver’s licence but asked with the law-enforcement Overlay it would flag the activity as suspicious, warn you, and possibly even report the establishment to authorities.

### 4.3.11. Revocations & Expiries

Credentials in an SSI world are held – not necessarily owned. Much like a driver’s licence is held by a person, it is actually owned by the government agency that issued it. We need to consider what happens in various cases:

- **REVOCAION** – if a Credential is revoked, we need to understand what our Digital Wallet does – does it remove that item? Does it look for a replacement (a revocation of a driver’s licence may just mean that a newer version has been created)? Does it automatically get removed from our Digital Wallet?

- EXPIRY – similarly, some Credentials are of no utility past a particular time – such as concert tickets. Depending on what we decide is important our Digital Wallet may clean itself up (e.g. move expired tickets to a trash folder) or require us to keep things in order.

### 4.3.12. Offline Operations

Digital Wallets may need to be able to operate under conditions where portions or all of a network are unavailable. Where there is a critical need for operations offline, multiple pieces of information will need to be cached locally:

- Cached Issuer Information – As critical issuers are offline, Wallets will need to know what the latest state of their Issuing DIDs (e.g. Public Keys).
- Revocation Registries – These will allow offline use of Credentials with more trust than is currently available with physical credentials.
- State Information – Digital Wallets will maintain a state that is relevant for various interactions that are occurring offline and simultaneously online. Reconciliation of activities that occurred during a period of being offline will be crucial.

### 4.3.13. Keys and Secrets

At its heart a Digital Wallet manages various different cryptographic keys and other items that need to be highly secure. Managing the creation, rotation, and revocation of these is crucial to ensuring that our Digital Wallet remains secure. These aspects are crucial to ensure that our wallets remain safe and usable.

### 4.3.14. Secure Hardware Integration

A Digital Wallet must leverage secure hardware capabilities such as trusted execution environments, secure enclaves, hardware security modules, etc. The use of these modules increases the overall security of your Digital Wallet. A Digital Wallet that avoids the use of such hardware should be considered suspect. Further if there are secure libraries (e.g. certified FIDO U2F SDKs) they could be live-signed at runtime<sup>17</sup> to ensure that they haven't been tampered with.

### 4.3.15. Notification

One of the key uses of a Digital Wallet application will be to provide information for its owner - whether that is a person or an organization. Messages for using Credentials, signing transactions, etc. will require notification. Depending on the use case these notifications may need to be on device or integrated into messaging systems for dissemination.

---

<sup>17</sup> <https://www.wolfssl.com/fips-140-2-validations-secure-enclave/>

Notification use cases are becoming well understood with Android and iOS providing OS-level notification. Digital Wallets will have multiple notification modes – some of which may require rethinking about how they are handled:

- Receipts – message receipt, receiving Credentials and other items, etc. are fairly routine.
- Time-sensitive – where there is a need for the Digital Wallet owner to act in a timely manner (e.g. “press OK if you are talking to your bank.” or “Please authorize this wire transfer”). Signing or authorizing activities will likely need this time-sensitive capability.
- Modal – messages that need to interrupt the flow of any other activities with the Digital Wallet.

### 4.3.16. Backup & Recovery

Losing your wallet is no fun. We all get nervous when it happens. The questions immediately start flowing:

- will I find it?
- if I do find it will everything be in it?
- what did I have in it?
- how can I get all the cards and identity documents replaced?
- is someone using my cards and info to steal my “identity”?

Recovery from a lost wallet is painful – especially if we have been compromised through fraud and/or identity theft.

#### WARNING

*It is important to understand that a Digital Wallet differs radically from a Cryptocurrency Wallet. Typically a Crypto Wallet can be restored by using just a Recovery Key. The restoring is done by reading the blockchain/ledger of each cryptocurrency to rebuild a history of activities. With a Digital Wallet the vast majority – potentially 100% – of the data are not stored anywhere publicly accessible. The contents are typically pushed to a Digital Wallet by an Issuer. This means that there is nowhere to go unless you have made backups.*

In the digital world there are options evolving – but you need to make certain that you have all your bases covered. There are two key things that differ with a Digital Wallet from a physical wallet:

- if you have a backup and recovery plan, you can recover your Digital Wallet completely if you have the keys.
- you need the keys to unlock the backup – and to take it back over if someone has compromised it. This also means that if you have lost the keys you may never get your Digital Wallet back.

At least, that is the promise of the emerging Digital Wallet industry. No known examples show, in the wild, how someone can re-assert control of a stolen Digital Wallet. But there are concrete plans and protocols being developed that will allow for this. (See [6.4.9. Backup & Recovery](#)).

But what do we need to back up?

Fundamentally there are two things that you can lose – and which need you to have a Backup available in order to recover your Digital Wallet:

- the keys and seed that protect the Wallet itself
- an encrypted backup of your Wallet contents

If you have both of those you can likely recover your Wallet relatively easily. If you don't, you are in trouble. Be sure that each is backed up somewhere that you can trust and access.

### 4.3.18. Vault Support

Wallets can only hold so much – and it isn't great to carry it all. The ability to keep some items in other places for safekeeping is crucial. Much like in the physical world, we need to be able to move things to and from various storage areas: Vaults.

In the physical world we keep many of our assets with various “Vaults”. We keep our cash in banks (it's actually just a digital representation of a promise to provide you cash, but hey), stocks with financial advisors and broker/custodians, insurance policies, and many other places.

Why wouldn't we do this in the digital world? The pure “decentralize the world” community considers this anathema, but we don't all want the headache and worry that comes with holding everything.

Assuming we want to be able to move things from our Wallet into a Vault and from a Vault to our wallet, we need to make sure our Digital Wallet is capable of supporting a Vault.

In the R&D section (see section [6.4.10. Vault-as-a-Service](#)) we'll discuss more detail about what a Vault is and what we, as an industry, need to learn and develop to make these a reality.

### 4.3.19. Multiple Device Support

We often use multiple wallets in the physical world and use multiple devices that we can use as a Digital Wallet. The reasons for using multiple physical wallets are manifold:

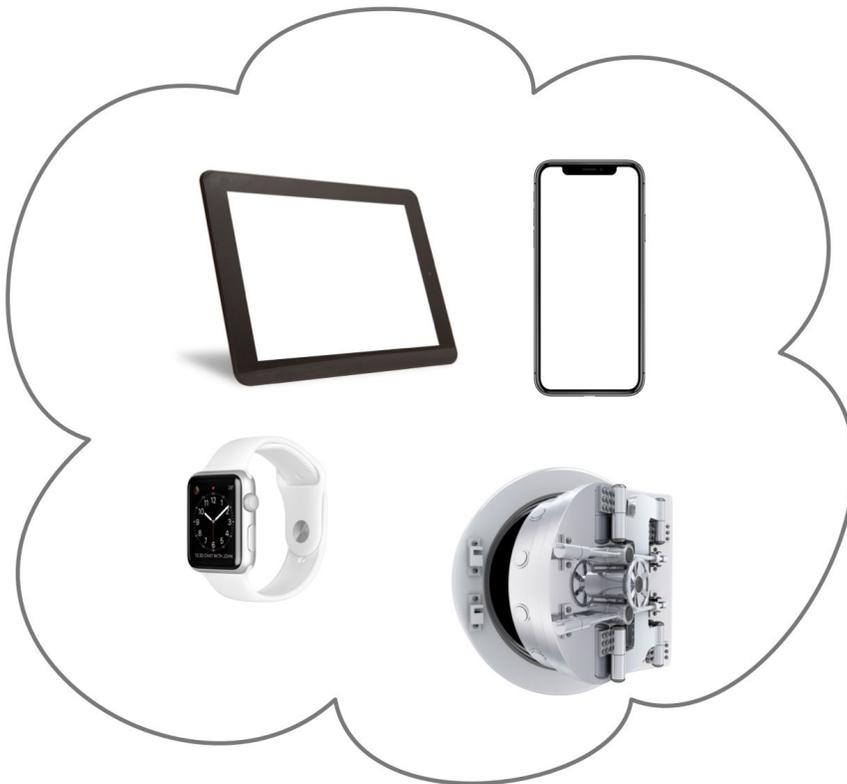
- travel vs. day-to-day – when travelling we may need our passports (en route) or want a completely minimal set of things (e.g. at the beach)

- style – the rugged carry-everything wallet doesn't always do the trick when you're dressed up
- purpose – some days a bank card and a driver's licence is all that is needed

The devices that we carry are similar. We may have a smartphone and a tablet that we use regularly. An officer in a company may keep company Credentials on a particular device that is kept under lock & key other than the times when is it used.

### 4.3.20. Synchronization

Key to supporting multiple Wallets is the ability to synchronize information between them and with any kind of vault storage. Carrying all things at the same time in each Digital Wallet likely doesn't fit the bill for usability. Some devices will be purpose-driven (e.g. corporate tablet for work; personal tablet for home) and others not suitable to carry too many Credentials.



As we look at where we will have Digital Wallets and the Vaults we see that there are many places where we will need our "Stuff". Similarly there are some devices where we explicitly do not want some Stuff. As examples:

- we may not want much information to be available on our smart watch
- we may want our recovery keys to only be in our Vault

- we may want to separate some key information between our smartphones and tablets – to ensure that we can recover if one of those devices is lost

Over time our Agents will get smarter and handle the synchronization that we need relatively seamlessly. For now this will be a very manual and onerous step.

#### 4.3.21. Selective Disclosure

Privacy-respecting credential usage means that an Identity Owner must be able to limit what information is shared with others. The ability to share limited subsets is called Selective Disclosure. Using attributes (aka Claims) from one or more Credentials allows a Person to decide what information they want to share.

<i>definition</i>	<b>Selective Disclosure</b>	<i>A Privacy by Design principle of revealing only the subset of the data described in a Claim, Credential, or other set of Private Data that is required by a Verifier. There are many techniques for achieving Selective Disclosure. One of the primary techniques used in Sovrin Infrastructure is Zero Knowledge Proof cryptography.</i>
	<i>[source if applicable]</i>	

The classic case of using a particular credential for multiple purposes can explain the utility of Selective Disclosure. Using a digital driver’s licence one can easily imagine the following unique presentations of the credential:

- Full Disclosure – present a full driver’s licence Credential, with all Claims exposed, to a law enforcement officer
- Partial – present a very limited portion for proof of “Age of Majority”. Alice presents only her picture and a binary value that says she is “over 19”. □

The use of Selective Disclosure, in the context of the above example, can benefit from overlays (see [Schemas & Overlays](#)). In the Driver’s Licence example we may have Overlays called Law Enforcement (full) and Age of Majority.

**WARNING**

*Many groups feel that governments can just issue multiple credentials at once, negating the need of Selective Disclosure. What isn't understood is that government agencies have extremely narrow definitions of what they are allowed to put into a Credential. In the case of a DMV, they don't have the mandate to issue an "Age of Majority" Credential. That's a different department/ministry – and the mandates are generally quite different. Selective Disclosure allows departments to focus on their mandate while allowing people to share appropriate information.*

### 4.3.22. Manage Guardianship & Delegation

Digital Wallet use implies that a person is fully able to perform all of the actions required to use it. What happens when a person isn't capable or willing to perform what is needed – and needs someone to act on their behalf? There are two main things to consider here:

- Guardianship – where we are explicitly acting on behalf of someone who can't act
- Delegation – where we are performing duties on behalf of someone because they have delegated the authority to us

#### DELEGATION

We don't do everything for ourselves. Often we have other people do things for us - because we have asked them to do so:

- pick up kids from school
- file our personal or corporate taxes
- guard our assets

#### GUARDIANSHIP

At other times in our lives there are needs for someone (an Identity Owner) to take over things for us – because we can't do them. This is where Guardianship comes in. Guardianship applies when a Dependent can't perform – because they are incapable or not allowed. Examples include:

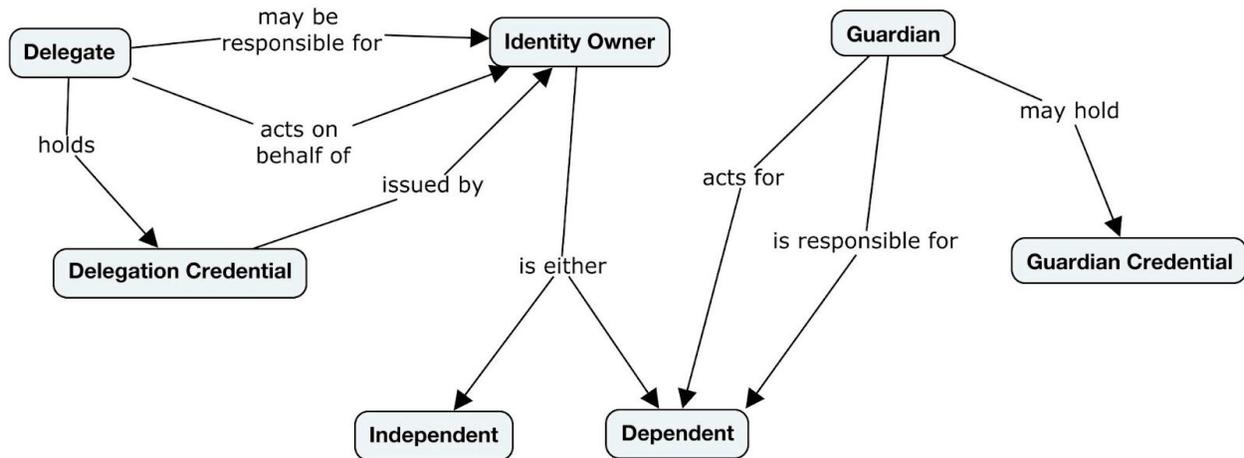
- parents acting on behalf of children
- an adult acting on behalf of a mentally or physically incapable person

On a technical level, the key difference between Delegation and Guardianship is control of the keys:

- under Delegation, both Identity Owners have a set of keys;

- under Guardianship, the Guardian is the only holder of keys. (Note: a Guardian needs to have 2 sets of keys – their personal keys and keys for the Dependent.)

Digital Wallets need to be able to handle these subtle differences. The use of Personas may assist in managing the complexity.



### 4.3.23. Messaging

In the physical world we ask each other for Credentials and other things that we hold in our physical wallets. In the Digital Wallet realm we need to parallel those messages:

- “Could I see some government identity?”
- “Do you have the receipt?”
- “Can you provide proof of address?”

These queries become much simpler when they are digitized – when someone needs your government identity to prove you are legally allowed to enter a drinking establishment, we can request things very specifically:

- we accept the following government Digital Identity Issuers – Ontario, British Columbia, and Alberta
- we will only use the “age of majority” Overlay as approved by each of those Issuers
- we will delete the information once we have logged non-identifying information

Codifying these digital interactions are crucial.

But those examples only show interactions that mimic how we use our physical wallet. The Agents in our Wallets can do far more.

- **Negotiate Payment** – an Agent can offer various payment approaches and currencies.
- **Consent Management** – an Agent can maintain a line of connection along with the consent(s) that go along with the relationship.
- **Approvals** – when the holder of the Digital Wallet needs to authorize transaction for themselves or others (e.g. under a Guardianship or Delegation case) digitally signed authorizations can be provided with ease.
- **General Communication** – Digital Wallets may provide a shared messaging capability that other apps could use for decentralized messaging.

### 4.3.24. Signing

The cryptographic keys in a Digital Wallet can be used to digitally “sign” various different digital items (e.g. contracts, messages). While this capability sounds abstract many of us are already doing this – when we use Apple Pay or Google Pay we are digitally “signing” the payments with our device. That device is tied to the biometric or passcode that locks our phones.

So what is different about a Digital Wallet? There are several key differences:

- **Who is Signing** – a Digital Wallet allows you to control which Digital Identity Artifact(s) you are using to sign things. This means you can have different ways that you sign different things. Imagine being an employee of a credit union that you have an account at – you may be signing things as an employee or as a member of the credit union. You can keep those separate in your Digital Wallet (see section [4.3.5. Personas](#)).
- It can provide you with the record of activities and keep documents that you have signed safe for you.
- A Digital Wallet can use zero-knowledge proof approaches to sign without needing to identify you directly.

When you are using your wallet to sign for transactions that only involve you, things are simple. However, when you are one of multiple people who needs to sign/approve something, your Wallet needs to handle a multiple signature (multisig) approach. Various cryptographic approaches will need support in your Digital Wallet.

## 4.4. Guiding Principles for Digital Wallets

There are a few high-level guiding principles that should be kept front of mind for those that are designing, building, and using Digital Wallets to create user experiences.

#### 4.4.1. Consent-Driven

2018 saw a major shift in consumer behaviour, with a relatively large portion of people realizing that social media and the “surveillance economy” were making them uncomfortable. Until the beginning of the Digital Wallet era, there haven’t been many alternatives. Experts like Doc Searls have envisioned a new way of sharing information where there is a “fourth party” that helps make sure that our information is treated well, and perhaps most importantly, shared with consent. These “fourth party” players are quite analogous to the Agents discussed in this report.

Digital Wallets play a role in creating the “intention economy”<sup>18</sup> and consent becomes a two-way process as opposed to the very one-sided process that it is now. A Digital Wallet will need to be able to provide the intentions – and give consent to those who are willing to play by the rules that our Agents enforce for us.

Consent-driven approaches to sharing information don’t need to be complex, but we need to have tools that make it simpler. Constantly being asked to consent to something that you obviously want to do is annoying. The Agents in our Digital Wallets can help maintain a balance between convenience and consent.

#### 4.4.2. Privacy by Design

A Digital Wallet is owned by a person. Sure, the software behind it was built by someone but the Digital Wallet – the software and the collection of stuff in it – is a personal asset. It is also likely going to contain information that is private. Applying the concepts of Privacy by Design<sup>19</sup> will be crucial. The [7 Foundational Principles](#) of Privacy by Design, created by Dr. Ann Cavoukian when she was the Privacy Commissioner of Ontario, provides high-level guidance that can help guide efforts in designing Digital Wallets.

The aspirations of the Privacy by Design principles often leave technical people looking for deeper guidance. Daniel Hardman and Jason Law of the Sovrin Foundation (and Evernym) provide excellent guidance in “[Self-Sovereign Privacy By Design](#)”<sup>20</sup>

#### 4.4.3. Security by Design

Digital Wallets should follow a “Security by Design” approach. Security by Design is still emergent and, unlike Privacy by Design, there are no rich resources to point at directly. The Sovrin Governance Framework is the best source to date as it focuses on the self-sovereign aspects which act in favour of the People and Organizations that hold the control of their identity

---

<sup>18</sup> Searls, Doc (2006-03-08). ["The Intention Economy"](#). *Linux Journal*. Retrieved 2007-09-28

<sup>19</sup> <https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/>

<sup>20</sup> [https://github.com/sovrin-foundation/protocol/blob/master/self\\_sovereign\\_privacy\\_by\\_design\\_v1.md](https://github.com/sovrin-foundation/protocol/blob/master/self_sovereign_privacy_by_design_v1.md)

documents. It covers the following principles (excerpted from the Sovrin Governance Framework<sup>21</sup>):

- System Diversity
- Secure Defaults
- Least Privilege
- Anti-Impersonation
- Auditability
- Secure Failure
- Pervasive Mediation

### 4.4.4. Portable and Open by Default

Past Digital Wallet efforts have failed for many reasons but the most common factor that impacted them was that they were created as closed systems. Closed systems have many faults but two major ones are:

- people are locked in and are unable to move to other systems
- vendors that are not part of the company or consortium are excluded and have no incentive to participate

The second factor (exclusionary team) has caused failures of Wallets since Microsoft Passport was released two decades ago. Though it continues to exist, it has devolved into an authentication capability used almost exclusively by Microsoft. Current Wallets like Apple Pay and Google Pay are more open – but still requires participating organizations to adhere to rules that they alone set.

The lock-in effect is more difficult to understand impact wise. When there is no ability to carry your information somewhere there is a natural resistance to investing too heavily – with our efforts and with our information.

Ensuring portability of the information contained in a Digital Wallet removes both of the factors that have caused failures. There are multiple solid examples of standards-based, portable systems that have created massive industries. The best example is the web browser industry which has enabled a multi-trillion dollar industry – based on common standards and portable information.

## 4.5. “Stuff” In A Digital Wallet

The earliest Wallets are holding a limited set of information. Mainstream Wallets like Apple Pay and Google Pay allow simple information to be “carried” inside them:

- credit cards

---

<sup>21</sup> <https://sovrin.org/library/sovrin-governance-framework/>

- tickets (e.g. plane tickets, event tickets)
- simple credentials (e.g. loyalty reward virtual card)

Over time more and more types of information will be useful in a Digital Wallet. This section briefly describes some of the capabilities that Digital Wallets are beginning to (or will) support.

A key aspect about a Digital Wallet relates to what it isn't. Though a Digital Wallet is a powerful concept it should not be considered to be "just a database" for things, nor as a cache of information. The way that a Digital Wallet needs to store and access encrypted data make it a terrible choice for both. It isn't meant to hold just about anything you can stuff into it.



Charles Kremenak, CC BY 2.0, Flickr

22

### 4.5.1. Receipts, Ownership, and Warranties

RECEIPTS – as purchases are made through or with a Digital Wallet engaged, the digital receipts can be stored. The richness of simple structured information in receipts – prices, item information – can build incredible information stores that are currently largely useless. Given the rich information that can flow during a transaction, new capabilities are available and a Digital Wallet can make a valuable tool. Some examples include how ownership and related warranties relate.

---

<sup>22</sup> Image source: <https://www.flickr.com/photos/charleskremenak/with/5986176148/> CCBy2.0

OWNERSHIP – consider each purchase that you make. Why doesn't your Wallet maintain a list of the things that you own? Currently there is a very indirect link between a receipt for payment and any formal registration of ownership, other than some key assets (e.g. real estate, vehicles, stocks). Most items – like a camera – don't have the explicit linkage of your purchase assigning the ownership. Sure the store maintains that a payment was made for a device – but it isn't logging the serial number of the device nor it is assigning explicit ownership over to you.

WARRANTIES – similar to ownerships, your Digital Wallet should be able to take the various things that you own and assign their warranties and other programs directly to you.

**STORY** - Avoid the "shoe box" problem

One of the problems identified with the various receipts that we gather over time (e.g. health care services, meals) is that we don't always get these things taken care of. The health insurance industry calls this the "shoe box" problem. Estimates are that the average Canadian loses over \$500 annually<sup>23</sup> because they forget to file various health insurance items that can be reimbursed. A Digital Wallet that has an Agent that monitors for various types of information (e.g. a Health Insurance Agent looking for eligible receipts) can take care of this problem.

#### 4.5.2. Address Book & Relationships

Our Digital Wallet will help us manage the connections that we have with various people and organizations. With private pairwise connections established with each party that we work with our Digital Wallet really becomes an ideal address book. Each relationship that we have can have rich information associated – and we may have many connections that jointly create a strong relationship to a person.

#### 4.5.3. Consent Receipts

As more and more privacy laws come into effect (e.g. GDPR in EU, California Consumer Privacy Act) the need to manage what we have agreed to share increases. A Digital Wallet, and the Agents that run as part of it, can help maintain the various different consent receipts<sup>24</sup> that pertain to what we share, when it can be used, and how we can sever or change our consent.

---

<sup>23</sup> "Avoid the Shoebox Effect — File Your Claim as Soon as Possible." Pacific Blue Cross Advice Centre. Accessed February 24, 2019. <https://www.pac.bluecross.ca/advicecentre/story/shoebox-effect>.

<sup>24</sup> <https://kantarainitiative.org/file-downloads/consent-receipt-specification-v1-1-0/>

## 4.6. Enterprise Wallets

### 4.6.1. Scale

Enterprise-grade Digital Wallets have requirements that are unique to managing the needs of an organization. Though some requirements may apply to People (e.g. scale) they become more important when worked at an enterprise level. There are several dimensions across which scale needs to be considered:

- **Multiple Entities** – enterprises will likely have multiple Wallets for various purposes (e.g. HR department, investor relations, corporate level) and will need to be able to use each Wallet in various ways. The existence of multiple entities within a larger entity introduces complexity that need to be considered.
- **Delegation** – corporations do not sign legal documents and act directly – the people they employ perform these tasks. Delegation and how it is managed and understood will be crucial for successful use of Digital Wallets. If a corporation has delegated authority for some legal issues to a partner in a law firm, there may be multiple Organizations and multiple levels of authority that need to be considered.
- **Performance** – corporations that are using Digital Wallets may need to do basic operations (e.g. provide a credential, validate a credential) at scales that eclipse what a person may ever do. While a Person could validate multiple Credentials within a few seconds (e.g. checking a contractor's insurance and training are current) a corporation may do thousands or more in the same time period.

### 4.6.2. Multiple Agents

Enterprises are more likely to have multiple agents – even of the same type – operating in the context of a single Digital Wallet.

Corporate functions requires oversight and notification in order to be able to operate large enterprises as a cohesive entity. As an Organization (or department in an Organization) grows, it may want to consider the use of Agents in the corporate Digital Wallets to help manage the complexity. We can imagine Agents that perform various duties:

- **Accounting & Finance** – management of payments, transactions, receipts, expense, approvals, and reimbursements will likely create its own industry of tools that can be used to get a handle on the finances of an enterprise. It is quite likely that a Corporate Expense Agent could be attached to an employee's Digital Wallet as well.
- **Compliance** – the transactions that a business unit conducts may require multiple groups to have compliance monitors attached to various Wallets.

- **Operations** – as more and more business is conducted with Digital Wallets, the operations of an Organization can be streamlined. Operations groups can attach themselves (as Agents) to various Digital Wallets
- **Inter-Entity** – Organizations thrive when different parts of the organization can share trusted information faster. As Digital Wallets evolve, key events (e.g. “contract signed”, “purchase order received”) can be shared instantly with looser integration than traditional systems integration requires.

### 4.6.3. Delegation (Rights, Roles, and Permissions)

With a Person, delegation as discussed in [Guardianship & Delegation](#) is optional and arguably an edge case. Within an enterprise, delegation is a hard requirement for most activities since People perform the duties on behalf of the enterprise. Even where automated (or autonomous) software is performing a duty, the enterprise still needs to delegate various permissions, rights, or roles to the software. Delegation in the enterprise is thus unavoidable.

Enterprises need to consider how they will delegate authority for the various rights, roles, and responsibilities that will make their Organization(s) successful.

Digital Wallets can be part of the delegation process. In addition to logging delegated actions, they can hold credentials that:

- indicate what capabilities have been delegated to someone
- can be updated or revoked as needed
- provide cryptographic signing capabilities

### 4.6.4. Protection

When you think about some of the most protected items inside a large corporation you need to think about things like the corporate seals – which are often held in a physical vault for safekeeping. The reality is that forging a corporate seal isn’t hard but we put a premium on these important physical devices.

Your author believes that enterprises that adopt Digital Wallets will lead in many domains. Business opportunities are certainly one. Another is that they will lead in exploring the risks of using Digital Wallets – and they will want to mitigate as much risk as possible.

Protection of Digital Wallets, particular the master keys, will be crucial for enterprises. While delegation will allow risk to be compartmentalized (e.g. moving all but the highest risk items into other Wallets) enterprises need to consider how they can put the processes and tools in place to protect and use a Digital Wallet wisely.



## 5. Agents – Deeper Detail

We've discussed that a Digital Wallet is comprised of Wallet Storage and Agents. The Agents work on our behalf to make our Digital Wallet work for us. Initially Agents will be quite basic and our Digital Wallet won't be terribly exciting. As the adoption of Digital Wallets increases we will be able to deploy Agents that do more and more things for us. They will help take care of the mundane, protect us from error and threats, and generally improve our lives.

But we have a lot of work ahead with Agents. This section aims to provide us with a bit deeper view of where Agents can go.

### 5.1. Types of Agents

The general idea behind Agents is that they handle things for the Person or Organization that may be useful in many ways. Various different types of Agents will be created in time. Some examples are:

- **Messaging Agent** – handles messaging for us in various contexts ranging from the simplest credential messaging (accepting, offering, etc.) to full 2-way messaging along the lines of a peer-to-peer version of WhatsApp.
- **Privacy Agent** – keeps a lock on privacy-invading information being shared unless you want it to be (or need it to be – using a panic button or something) and who you will allow to access it.
- **Delivery Agent** – handles delivery of packages to you (it may even arrange to put the eggs in your fridge) while maintaining a secure perimeter so your private information doesn't leak.
- **Health Agent** – ensures that you're following the eating approach that you want to, taking time to exercise, and generally checking up on things and staying safe. In the event that something happens to you (e.g. you have fallen and can't get up) it may reach out on your behalf to your loved ones and/or medical authorities.
- **Home Security Agent** – watches your residence and responds to threat and non-threat events for you. If your insurance company needs to know that you are meeting your obligations (e.g. is the alarm actually on when you're away?) perhaps you could share that information for a reduced premium.
- **Data Use Agent** – Sidewalk is building IP that will most likely drive a ton of revenue for Alphabet in the future. What if, as a resident, you could share in some of that revenue? A Data Use Agent would act on your behalf, ensuring you and your city get their fair share of revenue.
- **Buying Agent** – issues purchases on your behalf to vendors that are part of the ecosystem – this is your trusted fridge ordering your eggs and milk!

- **Marketing Agent** – blocks or allows marketing information to flow through to you. Not really a city-based approach but a key for local vendors to be aware of so they can know how to reach you, assuming you want that.
- **Reputation Manager** – handles your reputation scores on various different platforms that range from centralized (e.g. Uber, Yelp) to fully-decentralized systems that haven't even been deployed. The key here is that at some point you will own your own reputation data that other can use as input.

## 5.2. Who Is In Your Wallet?

The decentralization maximalists discuss removing any third parties from our lives. The general concept is that “middlemen” services don't add value and need to be disintermediated. The reality is that where a third-party is not adding value they will be removed – but what about the third parties that add value to our lives?

There is incredible value in allowing third parties “in” to your Digital Wallet – under your conditions, with full knowledge, and hopefully, with protection from them behaving badly.

Consider how the following scenarios can help in your day-to-day life:

- **Telco** – your smartphone is tied to your telco so it makes sense for them to play a role in helping you use and protect your Digital Wallet. Telcos will need to put deep processes in place to ensure that social engineering attacks are avoided.
- **Bank** – provides custodial services for your information and your digital assets. Banks, credit unions, and other financial institutions have been safeguarding assets for hundreds of years – and they have a role to play today and in the future. We rarely want to carry everything that we own with us – it's just too dangerous. Simple mistakes could mean the loss of all assets – with no recourse.
- **Insurance** – the contents of our Digital Wallet and how we use them raise questions of liability and risk. In time, the insurance market will characterize the risks and provide insurance. Examples may include insurance to confirm that key credentials are accurate and useful in particular cases (e.g. signing contracts with a rich credential backed by an insurance policy that says you really are you.)
- **Family & Friends** – we may want our family and friends to play various roles in our Digital Wallet. Whether that is for convenience (e.g. help recover keys) or requirement (e.g. authorizations for children that aren't of age) there are many different ways that we can interact. We may just be helping someone take care of a few things (e.g. protect a friend from phishing scams by being part of a multiple signature approval for wire transfers over a certain amount).
- **Health/Medical/Wellness** – the health information that we can store in our Wallet is incredibly valuable – directly for our own benefit and indirectly in service to society. If we are going to share information we need to know who we are sharing with, what they are allowed to see and do, and how we benefit.

### 5.2.1. Emergencies – Break Glass In Case of Emergency

Some health systems compartmentalize key information that can be accessed without express consent of the individual. We can call this capability the “break glass in case of emergency” features. However, they are hosted in the centralized systems that sit behind controls to protect that information.

A Digital Wallet will hold crucial information that may be useful in the event of an emergency. Various types of information can be compartmentalized and made accessible through various methods under various conditions such as:

- medical emergency – first responders and medical personnel/institutions will need access
- death or incapacitation – would potentially require legal intervention and consideration of legal authority

As more and more information moves to the edge of the networks and is under our direct control – in our Digital Wallet – the protocols in place do not work. I hold the information in my hand that used to live only in a centralized system.

We need Agents to help us ensure that the right people get the right information from us - without revealing too much to the wrong people. The Agents running in our Digital Wallets can do many things to ensure that the people requesting our private information have a bona fide right and requirement to use it. Similarly we need to ensure that if they don't have a Digital Wallet for ours to talk to, we may need to go fully manual.

### 5.2.2. Insurers

Earlier we hinted at the idea of an insured credential that we can use for signing contracts - where the insurer offsets the risk that someone is posing as you. There are many other cases where insurers may be deeply involved in your Wallet. These range widely:

- Insuring key digital assets from theft – an insurer may act as a third-party that helps to protect you in case your Wallet is stolen. They can block and potentially even reverse key actions (e.g. transfer of a particular asset that goes into 48-hour escrow account that can be interrupted in case of Wallet theft/takeover).
- Handling your receipts – as you accumulate receipts that are covered, they can automatically reimburse you.
- General liability – the use of a Digital Wallet means you are trusting the Wallet provider - but what if the builder of your Wallet had nefarious motives?

### 5.2.3. Monitor / Auditor

There are times when your Digital Wallet should actively intervene to keep you aware of activities and possibly notify authorities. A couple simple examples can help explain this concept:

- Age of Majority violation – imagine a time when you are used to providing a digital identity credential to enter a drinking establishment. They should normally use an overlay that asks for proof you are over a certain age and that this is you (perhaps a low-res picture of you). But what if they ask to see your full Digital Identity Document – much like a law enforcement official would? A Monitor could notify a government (or other) authority that the establishment is overreaching.
- Reputation Services – over time Digital Wallets will allow us to look at a broader picture of a Person or Organization’s reputation. You may want reputation services to look at, in a privacy-respecting way, the reputations of the people that you are dealing with. Additionally we may want to actively participate in such services – building our own reputation up.

## 6. State of Tech / Art of The Possible

### 6.1. Current Successes

The majority of successful Digital Wallet implementations reflect single-use scenarios.

- Crypto Wallets – allow sending and receiving of cryptocurrency.
- Ticket Apps – many airlines, hotels, and more use a basic Digital Wallet embedded in their applications to show tickets with QR codes and other ways to recognize a simple credential that represents a ticket.
- Loyalty Cards and Vendor Apps – vendors (e.g. Starbucks) have been very successful in creating credential-based versions of their cards and accounts. Very few, if any, are based on any standards beyond using QR codes for validation.
- Payment Cards – both the iOS and Android ecosystem have built in payment approaches. The Android “Wallet” (e.g. Google Pay)

More generic Digital Wallets exist, with the most successful being Apple Wallet, Google Pay, and Samsung Pay. It allows storing and display of multiple types of Credentials – though none are standards-based:

- Payment Cards
- Loyalty Cards
- Tickets/Passes

These more advanced Digital Wallets are beginning to adopt user experience strategies to make them more useful. As an example, travellers are now seeing that their boarding passes are showing on the lock screen. This is usually based on a time value and is a mediocre experience at best<sup>25</sup>. Other strategies such as integration with location-based information, NFC<sup>26</sup> and similar approaches will help here.

### 6.2. Where Are Things Working (and Failing) Now?

Considering the Digital Wallet space is over twenty years old, it has had very few solid successes. Such a fact needs to be considered by any organization or person that intends to build a business based on a Digital Wallet at its core.

---

<sup>25</sup> During this study your author had business travel issues when a 10:30am flight pass disappeared as it had been delayed until 7:15pm.

<sup>26</sup> Already part of Apple Pay and Google Pay but not for many non-payment credentials

Let's examine the current areas where Digital Wallets are working and discuss, at a high-level, how well they are working.

- **Payments** are increasingly popular though still a very small market with less than 3% of eligible transactions<sup>27</sup>. Apple clearly has the financial capacity to play the long game here and we can expect it to continue.
- **Loyalty Cards** are being used well in Digital Wallets. They are simple and don't have a lot of features but they make it easy to stop carrying numerous loyalty cards from vendors. That being said, your author still uses the Starbucks App to pay for things even though he could use the loyalty card in his Apple Wallet.
- **Tickets** have been used successfully by various airlines, movie theaters, and other apps (e.g. Meetup). The easy ability to find a ticket in your phone's Digital Wallet has clear benefits for people. There are still issues though – finding the ticket is hard if you have more than a few items in your wallet and getting rid of the old tickets is typically manual.
- **Cryptocurrency Wallets** have partially succeeded. They have taught people that digital assets can be secured. The amazing number of failures also provides a warning that the technology isn't everything and even that technology isn't as mature as it needs to be.

There are far more areas where the idea of a Digital Wallet is simply failing. These failures are partially due to the immaturity of technology but even more due to a misguided belief that technology alone is the solution. The list of areas of failure could take pages, so let's just look at a few examples:

- **Cryptocurrency Thefts** – there are weekly stories about personal and institutional cryptocurrency thefts. These failures are due to faulty processes (e.g. number porting process failures<sup>28</sup>), personal “security hygiene” failures, and insecure cryptocurrency wallets. These failures temper market demand by creating anchors for fear, uncertainty, and doubt.
- **Innovators Only** – Apple Pay is used in only 3% of eligible transactions. Why does it not get used more often? A major reason is that it is used by the innovators – a very small percentage of the population that adopts technology well ahead of everyone, including what we call “early adopters”. There is no coincidence that the percentage of Apple Pay transactions (< 3%) is very close to the percentage of innovators<sup>29</sup> in general society (~2.5%).

### 6.3. Where Is It Really Hard?

This report opened with statements that predict that Digital Wallets will shake the foundations of many industries.

---

<sup>27</sup> <https://www.pymnts.com/apple-pay-adoption/>

<sup>28</sup> [https://motherboard.vice.com/en\\_us/article/pawwkz/bitcoin-investor-sues-att-23-million-sim-swap-hack](https://motherboard.vice.com/en_us/article/pawwkz/bitcoin-investor-sues-att-23-million-sim-swap-hack)

<sup>29</sup> [https://en.wikipedia.org/wiki/Diffusion\\_of\\_innovations](https://en.wikipedia.org/wiki/Diffusion_of_innovations)

We can't expect that this will be easy. There are fundamental areas where the Digital Wallet space is either facing or will face difficulties. As a starting point consider the following:

- The **User Experience** for Digital Wallets is incredibly difficult. The long list of capabilities required, user interaction, user journeys, security and more impose extreme difficulty. The initial success for Digital Wallets will be laser-focused on very specific use cases and people may have no idea that they are using a Digital Wallet.
- **Keeping It Safe** (Loss and Theft Protection). Digital Wallet capabilities are increasing and the amount of Stuff we keep in them is growing. The pain of losing the contents of our Digital Wallet is increasing. Though people outside of the cryptocurrency Wallet space may understand, the general market does not “get” that their Digital Wallets need to be kept safe – and that means we need to lean on processes, organizations as well as tools<sup>30</sup> that can help us protect our Digital Wallet.
- **Driving Adoption** of Digital Wallets is difficult. A Digital Wallet is not a “first order” problem that people need to solve. Nobody wakes up and says, “Gee – I need a really good Digital Wallet”. What they do need is easier, safer, and even delightful ways to get things done in their lives.

## 6.4. Further Research and Effort

At this point we recognize that Digital Wallets are in very early stages. Research, Development, Education and other efforts are required to help move the Digital Wallet ecosystem forward. A few concepts are explored here.

### 6.4.1. Trust Hubs

In order to “trust” the various credentials that end up in a Wallet we need to be able to know that the Issuer of the credential is trusted in the first place. Every credential is created by an Issuer – so knowing how that Issuer’s authority is established is crucial. Otherwise a crafty teenager will create a DMV that issues driver’s licences which “look real” (i.e. the Credentials validate cryptographically and have data that make sense). They may even create a fake website that fools folks. But with the concept of a Trust Registry their efforts would fail.

We'll get to a more detailed description of a Trust Registry but in this case all that a law enforcement officer's Digital Wallet needs to know is the list of official DIDs from each province/state/federal authority that it recognizes – a very short list that doesn't change.

In order to get lists of the Issuers (e.g. the real DMV) a Wallet will need to be aware of the concept of Trust Registries (aka Trust Hubs).

- The concept behind a Trust Registry is that a Wallet needs to know which decentralized identifiers (DIDs) to “trust” as a source of truth. At many levels this “trust” translates to “authority” – knowing that there is somebody, centralized or decentralized, who is responsible for maintaining a list of trusted DIDs.

---

<sup>30</sup> The order of “processes, organization, and tools” was chosen very intentionally.

A Wallet will need to know which Registries are to be trusted. Over time the community will need to have Trust Registries that are anchored by various means:

- Legislative Authority – many Vital Statistics and other government Issuers. They are authoritative due to their legislative authority. Examples of these include issuers of: driver licences, hunting permits, building permits, passports, etc.
- Community Authority – some Trust Hubs will be created by communities, associations, etc. that exist through either a formal (similar to legislative) or de facto authority. Examples include: registry of licenced doctors; registry of banks and credit unions; industry associations, local business improvement areas/chambers of commerce; etc.
- Informal Authority – a Trust Hub should be able to exist with no formal authority. As an example, we can imagine consolidated reputations (E.g. Uber & Lyft combined; Yelp and TripAdvisor) that allow someone to aggregate reputation across platforms. It likely derives its authority from the larger community that “lends” reputation to them.

**Web of Trust** – the Owner(s) of a Wallet need to know that their Wallet is using the correct list of Trusted Issuers. Therefore a Wallet needs to be able to “explain” how it created the levels of Trust – and what anchored these trust levels. We can imagine the following chain of actions when we, as a homeowner, receive a bid folder from a renovation contractor:

- We check our contractor’s business licence which is anchored back to the province/state corporate registry.
- We check their insurance certificate against a list of Issuers on a nationally maintained list of insurance companies – a trust registry. That list is anchored back to various different province/state/federal registries that are the “source of truth” for insurance company establishment – another trust registry.
- We check the training status of all of the company’s workers as they arrive, to know that they have all the required certificates and training for the jobs that they are doing.
- We check the city to make sure that our contractor is licensed to operate. The city maintains a trust registry of businesses. We back-check the city licence bureau against their master list of Issuer DIDs. The city itself has a master DID that signed that registry and it points back to its legislative source of authority and the master list of municipalities for that province/state.

<i>definition</i>	<b>Sovrin Web of Trust Model</b>	<i>The decentralized, non-hierarchical trust model defined by the Sovrin Governance Framework that combines a cryptographic trust layer achieved using the Sovrin Ledger, Agents and Connections with a human trust layer achieved</i>
	<i>Sovrin Glossary</i>	

*via Credential Exchange. The Sovrin Web of Trust Model does not rely on a single root of trust, but empowers any Sovrin Entity to serve as a root of trust and enables all Sovrin Entities to participate in any number of interwoven Trust Communities, either informally or as defined by Domain-Specific Governance Frameworks. See the Sovrin Web of Trust Model white paper.*

That sounds like a lot of work doesn't it? Here's the thing – **we don't have to do any of this ourselves**. Our Digital Wallet should do this for us.

**STORY:** A Home Renovation...

Let's imagine a home renovation project with three main groups to think about:

- Homeowner
- Contractor
- City Inspector

Trust Hubs and Trust Registries allow us to know that the various credentials that are shared (e.g. proof of insurance) are real. A Homeowner can ask their Digital Wallet to verify an insurance Credential that the Contractor is real. Their Digital Wallet needs to prove a few things:

- That the Contractor was the entity that the Insurer (the Issuer) gave the Credential too. This is done inside the Contractor's Digital Wallet – it uses cryptography to prove that they still control the insurance Credential.
- That the Credential was cryptographically signed by the Insurer. This allows the Homeowner to know that the information wasn't tampered with.
- That the Insurer is a bona fide insurance company. There will need to be a Trust Hub that lists insurers for a particular area for this to happen.

All of the above can be done in just a few seconds and while that is being done other checks can be made. Each party involved has their own pieces of information that they need to verify.

- Homeowner wants to know that they have the right permits and licences for the job and that their contractor and the employees of the contractor are fully licensed, insured, and up to scratch.
- Contractor wants to know that the Homeowner has the right permits, licence, inspections and insurance.
- City Inspector wants to know that both the Homeowner and Contractor have the required permits, training, and other paperwork in place.

Paper-based approaches to verifying the above take long enough that few Homeowners ever do the checks that they should. Our Digital Wallets can get all of them done in seconds – even while we are greeting each other.

#### 6.4.2. Credential Lifecycle

When a Credential is issued the Issuer can't just forget that it was sent out – at least not in most cases. There is a lifecycle that needs to be considered. There are many different types of credential lifecycles to consider:

- **Fire and Forget** – some Credential lifecycles can, contrary to the opening sentence, involve simply issuing a Credential and never thinking about it again. Verifiers just confirm validity of the signature and they are done.
- **Revocable Credentials** – some Credentials are issued once and may be revoked later. An example would be a one-time pass that is used up (e.g. kind of a coupon). The verifier needs to know if the Credential is valid (i.e. has not been revoked).
- **Updated Credentials** – many Credentials need to be updated for various reasons. An example is a valid driver's licence that needs to be updated for a change of address. The Issuer will need to revoke the original Credential and replace it with a new one. A Verifier that looks at the original Credential may need to be able to understand that the revoked credential has been replaced.
- **Expiring Credentials** – a Credential that has a time limit is quite normal but there is little standardization about how that works in a Verifiable Credential realm. Additionally, it is common for an expiring Credential to be replaced by a new one that may create a dual valid Credential scenario (e.g. new credit card received before the old one expires).

Each of these lifecycles – and there are likely more – needs further R&D and education to ensure that People and Organizations understand how they work in detail. The subtle differences in these lifecycles are crucial to get right. Further, this effort can help standardize processes.

### 6.4.3. Certification

We pretty much agree that a Digital Wallet is going to be in our future.

Capabilities will range wildly and we will likely have a combination of different Agents that do things for us.

But who will make that Wallet? How do we know that we can trust it?

#### 6.4.3.1. Can We Trust Bubba's Wallet?

Imagine that Bubba's Wallet is ranked #1 in the app store. Can you trust it?

The short answer is **maybe**...

We need to figure out how to digitally sign an app (Bubba's Wallet) – so we know that when we run it, we aren't running a hacked version. Many pieces of the app need to be certified – the application developer; any libraries they use that are core to a Digital Wallet; and any certifications that the developer holds – so we can know that our Digital Wallet is safe to use. The groups (e.g. bank, government) that we share information with and get information from need to know that our wallet is trustworthy as well.

Digital signatures of an app are fine for general use. But a Digital Wallet is going to need a lot more behind it than "I, the developer of this beast, used my app store key to submit it." That developer could very easily be monitoring inputs and outputs for nefarious reasons. We need assurance that the application hasn't been tampered with and doesn't do bad things with our information.

#### 6.4.3.2. Certifying Bubba's Wallet

But how do we do that? That's where things get ugly potentially. We need to get into some pretty hard-core certification and accreditation. Some trusted third party needs to run through the application and make sure, to some high level, that it isn't doing nefarious (or stupid) things. That's going to cost money – a fair bit.

Is that fair though? Is it fair to ask Bubba, the masterful developer of Bubba's Wallet, to pay a third party \$5,000 to certify his application? What if the amount is \$50,000? \$250,000? Higher? Regardless of the cost, there will be some kind of certification regime – a "certified by \_\_\_\_\_" logo that needs to go beyond the cosmetics. It will need to provide real-time "not tampered with" certification. There are many areas that require thinking:

- Is there a way to tie Bubba's Wallet into a smartphone's trusted execution environment to generate this "not tampered with" certification?

- Who are the players that can help get this kind of real-time certification done? It’s likely the operating system providers, hardware manufacturers, banking networks and telecommunication providers will need to step in. They provide infrastructure and business services that will require highly trusted Digital Wallet technology.
- When does the cost of certification get high enough that we stifle the innovation that we need in the Digital Wallet community?
- What Organizations should be doing the certification? Do they need government approval? (Yes. Government approval in a decentralized world is a concept that needs to be considered.)
- How do we provide a digital “seal of approval” and know that the software that runs the Wallet hasn’t been tampered with?

#### 6.4.4. Rendering

Credentials are largely just a collection of attributes called claims. The visual rendering of such simple data has largely been to provide a tabular list of key names and values.

These are not the most attractive of user experiences. To a non-technical person, the idea that a digital driver’s licence could be shown as a table of values like the following is ridiculous.

Key Name	Value
first_name	TEST CARD
last_name	SAMPLE
middle_name	
dl_number	1234562
issued_datetime	2012-11-30
expires_datetime	2017-11-30
restrictions	2
endorsements	1
dl_class	5
...	
checksum	#QTRAASDV



Above: Example Physical Credential<sup>31</sup>

Rendering is the act of translating digital data into something visual – taking that tabular data and making it look like something regular people can make sense of. This means taking some

<sup>31</sup> Source: Government of British Columbia

attributes and either hiding them (many look like nonsense to a human) or transforming the raw data into something that makes more sense.

R&D is required to understand many things:

- How can a Credential be rendered to look like it approximates an official paper or plastic credential?
- What information should be hidden from view? A Digital Identity Document may hold multiple images, for example – used for different purposes. A high-resolution image may be appropriate for official use and a lower-resolution image for visual display.
- How can you visually render a Credential while making it easy for a device to request a proof of the signed data?

#### 6.4.5. No Device/No Smartphone

The majority of Digital Wallet activity is best suited for Smartphones. That leaves out any people who don't have access to a Smartphone. This means that Digital Wallet capabilities could create an exclusion barrier for the demographics that don't have devices.

Research is needed to understand what options are available to those who don't have devices capable of being a full Digital Wallet.

#### STORY A Pseudo-Guardian

A special case needs to be considered as the Digital Wallet market unfolds. While some smartphone applications are beginning to take on full Digital Wallet capabilities there are intermediate steps being taken that may feel like they violate the idea that a person must have total control of their Wallet. One pattern has emerged that sits between a fully-hosted Digital Wallet (i.e. controlled by the host) and a Digital Wallet that is controlled by the identity owner. These intermediate solutions use cloud-hosting where the Company/Organization is hosting information on behalf of an Identity Owner. Until standards are in place, particularly for portability, this pattern will continue to present discomfort for many. There are many reasons for this pattern to have emerged:

- There are no fully functioning Digital Wallets yet – not at the level that are defined in this report at least.
- There are unknowns in the broad scale deployments of generic Digital Wallets – see [6.4.3.1. Can We Trust Bubba's Wallet?](#) for more on this one.
- Applications are focused on a very particular usage. As an example, a non-governmental organization (NGO) may host a cloud Wallet for a beneficiary where they are doing only a very specific thing – such as managing eligibility for a particular benefit. The NGO in this case is an informal Guardian.

- Mobile applications that are interfacing with back-end services need to seamlessly integrate while awaiting local (i.e. on smartphone) capabilities such as reliable backup and restore, agent-to-agent communications that support mobility). An expedient engineering choice here is to start with a Wallet that is effectively – through no official mandate – held under Guardianship.

The hope behind these Pseudo-Guardian use cases is that control will be handed over to the individual Identity Owners in time. Where that isn't happening we can expect challenges to be issued.

The challenge to hand over control may very well create new business capabilities. We can imagine asking an insurance company to “take care of this for me” and handing over a key set of information (e.g. receipts for major purchases of items in your house) – and that there are legal assurances that the insurance company will do things properly.

#### 6.4.6. Guardianship & Delegation

While the theoretical concepts behind Delegation and Guardianship are becoming understood, there are no working examples in the wild that perform with a Digital Wallet. Manual processes are currently in use all over and range from highly formalized through to completely ad hoc and informal.

Experimentation and learning is needed to deeply understand the key requirements that will enable Guardianship and Delegation use cases with a Digital Wallet. Many questions need to be answered.

Early R&D and experimentation is needed to understand multiple things:

- Impact – what processes, people, and technology areas of your world (personal or business) will be impacted if you use digital approaches for Delegation or Guardianship.
- Minimal Viable Use – what is the most basic use? Do you need to wait for the technology and process standards to make forward progress? (The answer is no.)
- Security – allowing a painful process to be automated may be the wrong approach. Friction in current Delegation and Guardianship processes may be a very important feature. Automating the process could make taking over a more attractive prospect.

There are some key questions that need to be considered:

- When are we acting on someone's behalf? As a Person? As an Organization?
- What mandate – legal or otherwise – are you operating under? How has the Person or Organization that you are acting for delegated their authority to you?
- How do you return control back to a Person?

- How do you take necessary control from a Person who is unwilling (e.g. under court order)? Further, can your Organization support such a requirement?

The following questions may help understand the current limitations of digital Guardianship (see [4.3.21. Manage Guardianship & Delegation](#) Guardianship and Delegation) – particularly in relation to a Digital Wallet.

- How can a court order be imposed on a Wallet that is in control of a Person who requires Guardianship? Imagine an ill person who has, according to a court ruling, lost the capacity to manage their affairs. What control would allow for this – or should it ever be allowed?
- How can you be assured that a Guardian has fully relinquished control of a Digital Wallet? If they are controlling some historic keys, can they use some recovery mechanism to re-assert control?
- How can a Guardian hand over all or some control to a Dependent – or to another Guardian? The cryptographic control points get complicated quickly here.

In order for People or Organizations to use Digital Wallets for Delegation we need to understand how certain things can be done – in a standard way. Whether the standard is formal (de jure) or informal (de facto) research is needed to understand the following:

- What is being delegated and how does a service that supports delegation express the “capabilities” that can be delegated? Then how does a person get those capabilities assigned (delegated) to them?
- What approaches fit best into a Personal or Corporate Delegation case?

### **PERSONAL DELEGATION**

- Can another party (Person or Organization) trust that I have delegated a particular capacity to someone else?
- How do I revoke something that I have personally delegated to someone else? What happens both technically and potentially legally – especially in cases where a delegated authority was in the process of being used when it was revoked?
- What liability is incurred by the delegate? Delegator? Acceptor of Delegated authority?

### **ENTERPRISE DELEGATION**

Most activities that have legal consequence for Organizations are performed by People. These People are acting on behalf of an Organization, in a delegated capacity.

- Are Delegations supported on a policy level – ranging from internal policies to fully formalized legislated policies?

### 6.4.7. Schemas & Overlays

The use of robust Schemas in the Digital Wallet ecosystem is crucial. Many factors related to Schemas need R&D:

- How do schemas get re-used in other Schemas? Imagine a “civic address” Schema that is robust and wanting to include it in a higher-level “record of known addresses” Schema.
- Where do we find the best Schema? Is there something like schema.org that can apply?
- How do we tell others that we support Credentials that have a particular Schema and how do we let others know what Schema our Credentials support? With a decentralized anchor system (e.g. Sovrin ledger for Sovrin; Ethereum for uPort), discovery is non-trivial.
- Are there registry approaches that can be applied to this new world of Digital Wallets?

Related to Schema is the emerging Overlays concept – where data are transformed for various purposes:

- Entry Overlay – allowing standardizing entry of information
- Informational & Label Overlays – allowing more human-readable viewing of attributes, including language translation
- Subset Overlay – allowing breaking out a subset of a larger dataset
- Sensitive Overlay – allowing specification of the sensitivity of particular elements
- Encoding Overlay – relates to information for encoding methods used on various attributes
- Format Overlay – provides data typing and formatting for better understanding of underlying data
- Conditional Overlay – allows logical presentation (ordering, hiding, conditional displays) of data
- Consent Overlay – provides consent-centric information about data

The Overlays effort requires substantial efforts to align it with existing data standards and to flesh out where there are truly unique capabilities. This early stage effort is commendable.

### 6.4.8. 2FA/UFA Use Cases

The tech industry is pushing towards not allowing usernames and passwords. The addition of second-factor authentication (2FA) or removal of usernames and passwords in favour of universal authentication factor (UAF) are both gaining momentum.

Most industry standard use (e.g. FIDO U2F/UAF<sup>32</sup>, OpenID Connect<sup>33</sup>) of authentication relies on either a hardware device (e.g. Yubico's Yubikey) or an application that relies on a centralized service (e.g. Google Authenticator). Early ideas of using standardized approaches for the use of a Verifiable Credential in a 2FA manner warrant future R&D.

In particular:

- Can a Verifiable Credential or the underlying connection be used in an OpenID Connect context – as either a 2FA or UFA implementation?
- What would be needed to receive FIDO certification for the use of a Digital Wallet with Verifiable Credentials? As either U2F or UAF?
- How does a Digital Wallet and Verifiable Credential apply to FIDO2/WebAuthn?

### 6.4.9. Backup & Recovery

Given the growing importance that our Digital Wallets will have, we need to be assured that they will remain simple enough to use regularly but are difficult to lose.

This means key management and recovery methods need to be robust, secure AND simple. Generally the security side of things doesn't jive with that – you can pick two of those factors and usually need to sacrifice the other. That's not necessarily true. R&D can help find ways to create protocols that allow us to know exactly which dimension we may be sacrificing.

The key concerns about your Digital Wallet are:

- **Loss** – when you have either lost the device that the Digital Wallet was on or access to the keys/seed that unlock it.
- **Theft/Takeover** – when your keys have been compromised and a nefarious actor has taken over your Wallet.

**WARNING**

Social Engineering – The number one threat, in your author's view, to the success of Digital Wallets in the long-term is ensuring that the processes for recovering a Digital Wallet are not suborned. If the processes are flawed the Digital Wallet becomes a target for takeover resulting in theft and/or destruction of the digital assets that are forming a larger and larger portion of our lives. R&D is needed to test out processes and then education is needed to ensure that people and organizations have simple and trusted approaches to keeping our Digital Wallets, and their backups, safe.

Wallet protection in general warrants further research, development, and education.

---

<sup>32</sup> <https://fidoalliance.org/specifications/>

<sup>33</sup> <https://openid.net/connect/>

Further, the management of the secrets and keys that are critical to using, protecting, and recovering a Digital Wallet are crucial. An effort that is worth pursuing is Distributed Key Management System (DKMS<sup>34</sup>).

#### 6.4.10. Vault-as-a-Service

In [Vault Support](#) we discussed that a Digital Wallet needs to be able to move information into and out of a digital Vault for safekeeping. The exact specifications of what a Vault is – beyond a simple place for backup – is not well known. The idea is early enough in some ways that the term isn't widely used in the self-sovereign realm – perhaps due to the focus on decentralization, while most Vault providers would be centralized in the beginning.

R&D is required to:

- Broadly define what a Vault is – what capabilities does a good Vault have? What does it specifically do and not do?
- Understand the processes and tooling needed to create digital equivalents of safe-deposit boxes? The physical protocols that block a bank employee from opening a customer's safe deposit box are crucial.
- Specify the protocols and governance required where Vaults are in use.

#### 6.4.11. Break Glass In Case of Emergency

As we use our Digital Wallets more and more the information in them will grow. Much of that information is private – which is how we'd like it to stay, until we need to share it but can't. Imagine an unconscious person whose phone contains information vital to ensuring first responders provide the best care possible. Protocols exist in many discrete places but few standards exist.

<b>Story:</b> Medical Nightmare Today, Security Nightmare Tomorrow
Let's imagine a scenario where I am traveling alone on business, in a foreign country. I had a cough that was bad enough to warrant going to the doctor. A day after landing in the foreign country I end up in medical distress and can't figure out what is happening but I know it is severe so I head to an emergency room. By the time I arrive I am in dire straits – in and out of consciousness.

---

<sup>34</sup> Reed, Drummond, Jason Law, Daniel Hardman, and Michael Lodder. "[DKMS \(Decentralized Key Management System\) Design and Architecture V3.](#)" 2017. Hyperledger, accessed February 22, 2019.

The medical staff don't have access to the "break glass in case of emergency" and I am in enough trouble that I am not coherent enough to provide good information to the medical professionals.

They hit my iOS smartphone and see that Medical ID is enabled. It tells them I have a peanut allergy.

But the reaction isn't at all consistent with a peanut allergy. They can't see that I just received an antibiotic and that I regularly take other medication. If they could they may realize that I am having an adverse reaction to combining medications.

They don't know who to reach out to.

So what do they do? Let's hope I don't need to find out.

BUT – what if my Digital Wallet could:

- Tell them the details above they could provide far better medical care. (The problem is if that is openly available to anyone who opens my phone up I am freaked out – we can't have total strangers accessing that much information.)
- Notify a designated family member that my medical details have been accessed – and have that logged somewhere (for abuse detection amongst other uses.)

There are a lot of questions and areas that need research here. Here are a few:

- Who are the authorities that get to break the glass?
- Can we create a system where credentialed authorities (e.g. certified first responders, doctors, nurses, hospital EHR systems) can access certain types of information without explicit consent?
  - What happens when the authorities are not in our ecosystem (i.e. they don't do VerCreds, etc.)?
  - How do we ensure that this isn't abused? What logging and auditability should our Digital Wallets perform? Should our Wallet notify a service when the "break glass" feature is invoked?

## 6.4.12. Bare Minimum Portability

A Digital Wallet may contain information that is vastly different from what another Digital Wallet may contain. Expecting each Digital Wallet to have the same feature set as others is not realistic. However, in order to have some portability we need to understand what the bare minimum capabilities of each Digital Wallet provider is. Research is needed to understand the following:

- **Wallet Capabilities** – What information can a Digital Wallet manage for us and what limitations are there?
- **Agent Compatibility** – Can the Agents that operate in different Wallets understand each other? Are there mechanisms by which data can be shared directly or via transformation?
- **Discovery** – What can be done to profile the various types of Digital Wallet that exist? Profiles can help people discover that there may be a Digital Wallet that could work better for them (e.g. imagine a Digital Wallet that focuses on the Diabetes Type II community).

## 6.5. Standards

The Digital Wallet ecosystem is in a very early stage where few, if any, standards exist. Neither informal (de facto) nor formal (de jure) standards exist in most areas – from the self-sovereign identity stack, through Wallet portability, Credential offer/acceptance/storage/retrieval, and beyond.

That doesn't mean there aren't areas where standardization efforts are warranted.

### 6.5.1. Protocol Evolution

As we look at the requirement for Standards (see previous section) it is clear that there is a need for **Standards and open protocols** to ensure that we're not being locked in to something and to share the benefits of learning broadly in the community.

The three main stages of a protocol are:

- **Isolated (or Proprietary)** – a singular implementation exists likely from a single closed- or open-source project and it has minor adoption in a very closed project or customer base
- **Community** – a larger community has begun to use some competing (Isolated) versions and realizes that they need to converge on a common protocol in order to grow as a community

- **Formal** – a group of communities have put in the effort to formalize a broad protocol, usually through a standards body of some kind (e.g. [IETF](https://www.ietf.org/)<sup>35</sup>, [OASIS](https://www.oasis-open.org/)<sup>36</sup>)

Most useful protocols start off as an **Isolated** use capability that can barely be described as a “protocol”. Over time, as it shows value there is a **Community** level adoption. If the protocol is truly valuable there is a push to create a **Formal** protocol.



### 6.5.1.1. Is It Worth The Effort?

At every shift there is a substantial effort to lift a protocol to the next stage. The efforts relate to:

- **Technical Development Efforts** – the technical community expends a large amount of time working on the common and different use cases, digging out the incompatibilities, breaking thing down to the bare minimums, and much more
- **Social Capital Investment** – the amount of social capital that is invested to push a protocol forward. This investment is crucial for success of a protocol

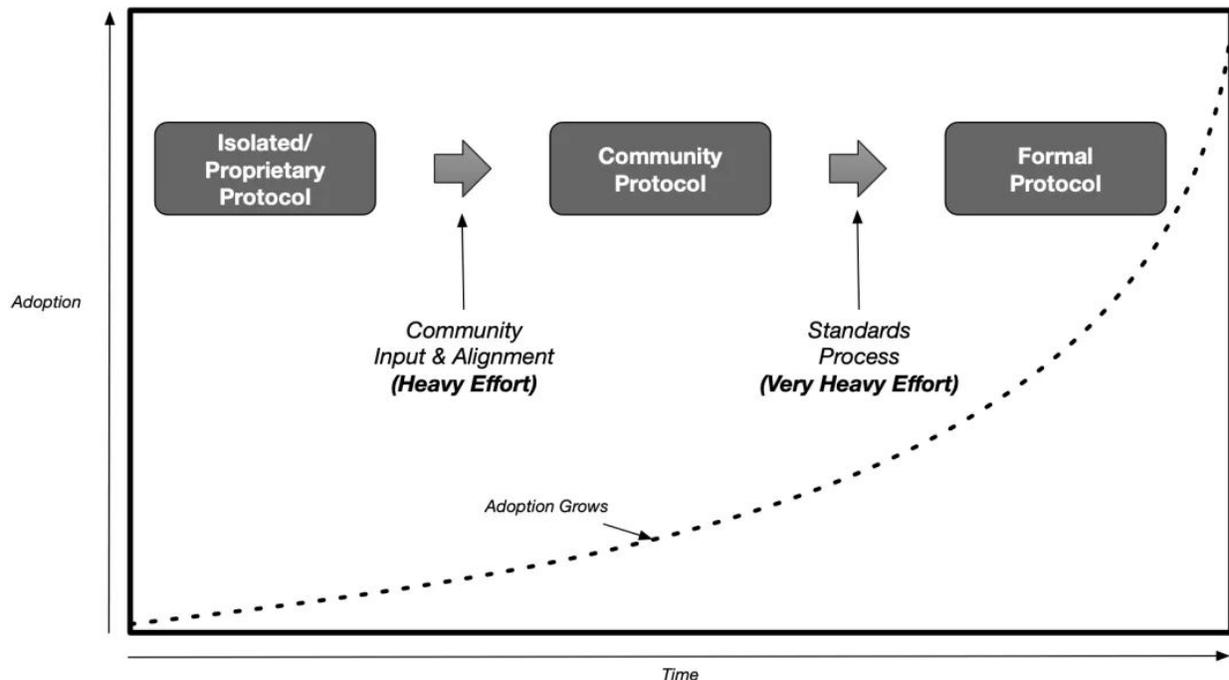
These efforts need to be gauged against results. If adoption doesn’t grow with more formalization there may be no need for a broadly applicable protocol. The successful protocols

---

<sup>35</sup> <https://ietf.org/>

<sup>36</sup> <https://www.oasis-open.org/>

drive adoption as they get more and more formal.



#### 6.5.1.2. A Small Example – Sovrin Agent-to-Agent

The Hyperledger Indy/Sovrin community provides a good example of the evolution of a protocol.

In the Sovrin community, initial efforts to establish protocols that enable Agent-to-Agent communication were focused on two key libraries – both donated by Evernym:

- **libIndy** – a low-level library focused on interactions with the ledger and low-level wallet storage capabilities.
- **libVCX** – a library that began handling Agent-to-Agent communications, Credential management, and proof requests.

Initially these libraries were completely proprietary, owned by a single company. These libraries were donated<sup>37</sup> by Evernym to the Sovrin Foundation and then by the Sovrin Foundation to the Hyperledger Project, part of the Linux Foundation.

Subsequently, many additional projects began to work on Agents, proving that a **Community Protocol** had begun to emerge:

- BC Government’s **VONx**<sup>38</sup> project

<sup>37</sup> “[Why We’re Investing In... Evernym & The Sovrin Foundation](#) | ” *Outlier Ventures | Investing in Blockchain, AI & IoT Tech* (blog), October 22, 2017.

<sup>38</sup> <https://vonx.io>

- [BYU](#) early reference agent<sup>39</sup>
- [Streetcred](#)<sup>40</sup>

In time the Sovrin A2A protocol will help drive for a **Formal Protocol** that supports a multitude of underlying systems. The investment required to take disparate communities (e.g. [DIF](#)<sup>41</sup>, [uPort](#)<sup>42</sup>, and [Veres.one](#)<sup>43</sup>) and shift to a formal broader community standard needs to be worthwhile though. The technical and social investment to do so are quite large and it will take time. Anyone basing business and short-term decisions on a **Formal** protocol should look for **Community** (or **Isolated**) protocols that meet their needs for now.

### 6.5.2. Overview of Standards Landscape

The Digital Wallet space is going to require standards for interoperability and assurance that the Digital Wallets we use are fit for purpose and safe to use. Standards and certifications are woefully missing from the Digital Wallet landscape at this time.

Standards are required at many levels:

- **Self Sovereign Identity** – while early efforts at defining “the stack” have begun, there are few if any efforts that are producing community standards, let alone formal standards.
- **Key Management** – the ability to manage (create, rotate, and recover) the keys to your Wallet are a crucial standard. Efforts are underway to bring the DKMS approach to a standards definition organization (e.g. OASIS) but these are early days.
- **Portability** – there are no standards in play at time of writing, though proprietary approaches are emerging.
- **Guardianship** – guardianship is going to require many different standards to ensure that it can be supported broadly under the many contexts where it applies.
- **Delegation** – the ability to either delegate control to someone for a specific task (e.g. sign contract with value less than \$10,000) requires understanding of the data exchanges, information flows, and the standards that are applied.
- **Certification** – the value of information in our Digital Wallets is increasing. We need to know that we can trust the application providers. The parties we share information with also need the same assurances. Over time there will be certification and accreditation regimes placed. Governments may provide a key role in mandating and guiding the certifications that are required.
- **Trust Hubs** – no formal standards exist for managing the lists of “official” credential issuers but informal efforts have begun.

---

<sup>39</sup> <https://github.com/hyperledger/indy-agent/tree/master/nodejs>

<sup>40</sup> <https://github.com/streetcred-id/agent-framework>

<sup>41</sup> <https://identity.foundation/>

<sup>42</sup> <https://www.uport.me>

<sup>43</sup> <https://veres.one/>

Some areas already have standards in place that our Digital Wallets can work towards:

- **Authentication** – the FIDO Alliance Standards (U2F, UAF, and FIDO2) and OpenID Connect, W3C (WebAuthn), and others provide frameworks that our Digital Wallets can integrate and support.

Overall for any Organization that expects formality and rigid standards, the Digital Wallet ecosystem is way too early to consider.

### 6.5.3. Assurance Levels

Determining assurance levels requires an understanding of the difference between Identity Assurance (a measure of certainty that an Individual, Organization or device is who or what it claims to be) and Credential Assurance (how can we be sure it is them once we have identified them?).

<i>definition</i>	<b>Identity Assurance</b>	<i>A measure of certainty that an Individual, Organization or device is who or what it claims to be.</i>
	<a href="#">TBS</a>	
<i>definition</i>	<b>Credential Assurance</b>	<i>The assurance that an Individual, Organization or device has maintained control over what has been entrusted to him or her (e.g., key, token, document, identifier) and that the Credential has not been compromised (e.g., tampered with, modified).</i>
	<a href="#">TBS</a>	

Two major pieces of guidance apply for the purposes of this report – aimed globally but where required, focused on Canadian and US particulars.

- **NIST 800-63** – US Standard provides deep technical details in IAL and AAL and will be most helpful for security and IT analysis.
- **Treasury Board Secretariat Canada (TBS)** – provides a more business-focused and citizen-centric approach to IAL and AAL. Business users will likely get more from the

information. It provides more of the “why” than the “what and how” that NIST 800-63 provides.

At a business level the TBS and the draft Pan-Canadian Trust Framework (PCTF) provide much more useful input, while the NIST standard is extremely technically detailed.

### 6.5.3.1. Identity Assurance Levels

Identity Assurance Levels allow us to understand what assurance we can place in the Identity Proofing processes that are in place. Understanding that a Person has been correctly identified underpins all future identity-related transactions. This process is what Identity Assurance is all about. Basically, can we trust that a Person has been proved to be who they say they are – to a certain level of assurance.

<i>definition</i>	<b>Identity Assurance Level</b>	<i>The level of confidence that an Individual, Organization or device is who or what it claims to be.</i>
	<a href="#">TBS</a>	

As an example we’ll look at the TBS and NIST Identity Assurance Levels for comparison. As mentioned earlier they take different approaches, with TBS being more descriptive for business use and NIST being more technical.

#### TBS Identity Assurance Levels

Level	Description
<b>4</b>	<b>Very high confidence required that an Individual is who he or she claims to be</b> Compromise could reasonably be expected to cause serious to catastrophic harm
<b>3</b>	<b>High confidence required that an Individual is who he or she claims to be</b> Compromise could reasonably be expected to cause moderate to serious harm
<b>2</b>	<b>Some confidence required that an Individual is who he or she claims to be</b> Compromise could reasonably be expected to cause minimal to moderate harm
<b>1</b>	<b>Little confidence required that an Individual is who he or she claims to be</b> Compromise could reasonably be expected to cause nil to minimal harm

**NIST 800-63 Identity Assurance Levels:**

- **IAL1:** At IAL1, attributes, if any, are self-asserted or should be treated as self-asserted.
- **IAL2:** At IAL2, either remote or in-person identity proofing is required. IAL2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in [SP 800-63A](#).
- **IAL3:** At IAL3, in-person identity proofing is required. Identifying attributes must be verified by an authorized CSP representative through examination of physical documentation as described in [SP 800-63A](#).

6.5.3.2. Credential Assurance Levels

<i>definition</i>	<b>Credential Assurance Level</b>	<i>The level of confidence that an Individual, Organization or device has maintained control over what has been entrusted to him or her (e.g., key, token, document, identifier) and that the Credential has not been compromised (e.g., tampered with, corrupted, modified).</i>
	<a href="#">TBS</a>	

TBS provides a 4-level system for classifying Credential Assurance Levels. It’s plain language speaks of compromise impacts, which helps business analysis.

**TBS Credential Assurance Levels**

Level	Description
<b>4</b>	<p><b>Very high confidence required that an Individual has maintained control over a Credential that has been entrusted to him or her and that the Credential has not been compromised.</b></p> <p>Compromise could reasonably be expected to cause serious to catastrophic harm.</p>
<b>3</b>	<p><b>High confidence required that an Individual has maintained control over a Credential that has been entrusted to him or her and that the Credential has not been compromised.</b></p> <p>Compromise could reasonably be expected to cause moderate to serious harm.</p>

<b>2</b>	<p><b>Some confidence required that an Individual has maintained control over a Credential that has been entrusted to him or her and that the Credential has not been compromised.</b></p> <p>Compromise could reasonably be expected to cause minimal to moderate harm.</p>
<b>1</b>	<p><b>Little confidence required that an Individual has maintained control over a Credential that has been entrusted to him or her and that the Credential has not been compromised.</b></p> <p>Compromise could reasonably be expected to cause nil to minimal harm.</p>

NIST provides an equivalent “Authenticator” (vice “Credential”) Assurance Level breakdown - using only 3 levels.

**NIST 800-63 Authenticator Assurance Levels:**

- **AAL1:** AAL1 provides some assurance that the claimant controls an authenticator registered to the subscriber. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator(s) through a secure authentication protocol.
- **AAL2:** AAL2 provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through a secure authentication protocol. Approved cryptographic techniques are required at AAL2 and above.
- **AAL3:** AAL3 provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a “hard” cryptographic authenticator that provides verifier impersonation resistance.

6.5.4. PCTF

Canada has been providing deep leadership in the Digital Identity space for over a decade. With its unique government structure and open approach, the world has rightfully been looking to Canada for ongoing leadership in identity. That leadership position includes a key piece of work that impacts Digital Wallets: the Pan-Canadian Trust Framework.

Private industry group, DIACC ([www.diacc.ca](http://www.diacc.ca)) is working together with government’s Identity Management Steering Committee (IMSC<sup>44</sup>) to create the PCTF. The goal of the PCTF is to

---

<sup>44</sup> IMSC was established in 2011 by federal/provincial/territorial governments in Canada (<https://iccs-isac.org/councils/joint-councils/identity-management-sub-committee>)

create a framework that allows citizens and business to rely upon Digital Identity to build a stronger economy and country.

At the time of writing DIACC had issued a draft PCTF Overview with requests for comment<sup>45</sup> and the IMSC provided a draft PCTF<sup>46</sup>. In time we hope that the two groups merge their capabilities into a comprehensive PCTF.

Recent input and [discussion documents](#) from Canadian government provide deep guidance about how the underlying processes and artifacts of identity can be used in a Digital Wallet.

The hope is that the PCTF will provide leadership and guidance in many areas that are directly relevant to the Digital Wallet space:

- define Trusted Processes that can be used as building blocks to create rich and secure systems
- look to use a Vectors of Trust approach to understand how much assurance we can place on the processes and artifacts that are used to create the Credentials that our Digital Wallet will hold
- link efforts to policy, regulation, and legislation - so we know why certain things are being done
- provide normalization so we can understand terms consistently across various sectors and ecosystems

The PCTF is currently being curated by an industry group that partners private and public resources. That venue should be able to produce a coherent plan for Canada.

### 6.5.5. Portability

In order to ensure that Digital Wallets are as useful as possible, they should allow for portability – meaning that you can change your Wallet provider with minimal effort and not lose information. Perhaps more difficult to define at this time is that loss of capability that may occur if you change Wallets.

If you have multiple Agents working in your Wallet, such as a financial monitor Agent and a health services Agent, what happens when you change Wallets? Does your current set of Agents work in that new Wallet? Are they functionally equivalent – or have you just broken things?

---

<sup>45</sup> DIACC. “Request for Review and Comment: PCTF Model Overview Discussion Draft V0.02 Review – Digital ID & Authentication Council of Canada.” Accessed February 23, 2019. <https://diacc.ca/2019/02/12/pctf-model-overview-discussion-draft-v0-02/>.

<sup>46</sup> “Overview of the IMSC PCTF Version 0.9 v0.1 (2019-02-20).Pdf.” Google Docs. Accessed February 23, 2019. <https://t.co/flpj1stNir>

Portability in Digital Wallets will initially be similar to the portability that social media companies currently support. While some groups think that data portability is valuable<sup>47</sup> there is a flaw in how things actually work. If you download your Facebook data you have access to the raw data – but what can you do with it? You can't just upload it to another site – there is nothing useful to it unless you are a data analyst. “Data Portability” of a Digital Wallet will be similar - but the hopes are that there will be a bare minimum of capabilities that Digital Wallets can do with respect to Portability (see section [6.4.12. Bare Minimum Portability](#) for more detail).

## 6.6. The User Experience Challenge

Overall the user experience (UX) for Wallets has been, with few exceptions, miserable to date. From Microsoft Passport over twenty years ago to the most current Apple Wallet and Google Pay, the experiences have not delighted.

Currently the successful actions that are happening with Digital Wallets actually don't feel like we are using a Digital Wallet. Using Apple Pay or Google Pay is simple – pass your smartphone over a device and biometrically approve the transaction. At no point do we actually “pull out our wallet”. Behind the scenes our Digital Wallet was talking to the payment terminal, negotiating, and facilitating the transaction. All the Digital Wallet needed from us was the biometric authorization.

The uses of early Digital Wallets are focused on very simple actions where the Digital Wallet is hidden from use. That is the user experience that is succeeding.

Your author has a Starbucks credential in his Apple Wallet. However, flipping to open the Apple Wallet, flipping through the 8-10 “cards” in it to load up the Starbucks “card” is painful. Instead he loads the Starbucks app, which is always in the same spot on his home screen, shakes it and pays. That's a UX failure as far as a Digital Wallet is concerned.

### 6.6.1. Organizing and Finding My Stuff

The hardest user experience initially is going to be the organization of all of the Stuff that I can put in my wallet. Like the classic episode of Seinfeld where George Costanza can't close his wallet due to all the cards and receipts that has in it, we will have a big problem. That problem is that it is too easy to put Stuff into a Digital Wallet. Once the Standards shake out, receipts, Credentials, and more will rapidly accumulate.

---

<sup>47</sup> O'Brien, Danny, and Bennett Cyphers. “[Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine.](#)” Electronic Frontier Foundation, July 24, 2018.

So how do you organize them – and can your Digital Wallet keep Stuff organized without accidentally hiding them from you? The organization side of wallets will likely take years to shake out.

Research is needed to examine the various user experiences that are needed to manage the growing information. UI approaches, categorization, automatic requests/offers, and many more areas need exploration. Interaction designers, UX experts, human factor engineers, among others, are also needed.

### 6.6.2. Invites, Offers, and Requests

A Digital Wallet that is empty isn't very helpful to anyone. We need to ensure that the ability to put things into our Wallet isn't incredibly hard or confusing.

Similarly we should be able to “take something out” of our Digital Wallet to offer it to someone else – much like we do in the physical world.

These actions should feel intuitive.

Some actions may just be built in and completely invisible. As an example, if we buy some movie tickets and arrive at the theatre, why would we need to dig around looking for the ticket? As long as the movie theatre knows how to tell the Digital Wallet what it needs or can use, our Digital Wallet can have things at the ready. A simple visit to the movies could involve a silent conversation as we walk in, where the theatre systems and our Digital Wallet “talk”:

- Theatre system: “Hi there! I am theatre XYZ – if you have any tickets or coupons for me that are valid now, I can help.”
- Digital Wallet: “I have two passes for a movie here starting in 25 minutes and a coupon for food.”

That simple digital conversation allows our Digital Wallet to be ready to present the tickets instead of digging into an application that we can't find easily.

Over time the movement of the “Stuff” in our Digital Wallet will largely happen in the background.

### 6.6.3. What's Normal (What's Weird)?

One key thing that our Digital Wallet will need to do in the future is to make sure that we are sharing what we should be. A stranger asking for a full passport profile will become an odd request in time and our Digital Wallet should warn us. Many of the warnings will likely relate to privacy, where more information is requested than is required.

What kind of “normal” activity will our Wallet allow us to do – and when will it flag us that something is not normal or even creepy. Let’s run through a few examples:

- **Semi-anonymous transactions** – many interactions in life are nearly anonymous and should remain so. Paying for something with cash is nearly anonymous and it is logical that similar capabilities will continue to exist in the digital realm. But some transactions require a bit more, e.g., proof that a person is old enough to make a particular purchase. Our Wallet, using selective disclosure and zero-knowledge proofs, can do this. It can also warn us when more information than is required is being requested.
- **Surveillance** – Digital Wallets should establish unique (pairwise) connections with each party we work with. As a relationship is totally unique we can understand how often it is requesting information, what consent we have given, and more. This information can make a digital relationship very healthy or can indicate that it is being abused. As the Agents in our Digital Wallets get “smarter” they will be able to tell us when we have a digital relationship that is going farther than we would like – and adjust or terminate that relationship.
- **Law Violations** – Some activities are simply not legal for various reasons that range from civil code violations through to fully criminal behaviour. Our Digital Wallets can protect us from inadvertently crossing a line that we weren’t aware of. As data moves through our pairwise connections, we can monitor them for nefarious activity. Asking for a full driver’s licence with name, address, date of birth, and more will become odd in time and at some point a jurisdiction will make requesting it illegal at some level.

The key action that our Digital Wallet will do here is warn us and stop us from doing things that just aren’t good for us. Of course, you should be able to do whatever you like – and your Digital Wallet shouldn’t stop you. However, you may have particular Agents in your Digital Wallet that only allow certain activities and actions.

## 7. Business & Markets

The Digital Wallet business market will form an ecosystem. Providers of Digital Wallet components will range from OS providers (e.g. Apple, Google, Microsoft), hardware platform providers (e.g. Apple, Samsung), and many software providers. As discussed in the prior section the ecosystem will evolve from discrete applications through to a more plug-and-play world where we have some freedom to pick pieces.

The market is very early though. The best way for Individual and Organizations are to consider the following approaches.

Let's discuss how the market will evolve and then some early approaches that can be used to take advantage of the evolving Digital Wallet space.

### 7.1. The Evolution of Digital Wallets

Like any ecosystem, the Digital Wallet space will evolve over time. The space will go through at least three stages:

- Stage 1 – Basic Digital Wallets
- Stage 2 – Specialized Applications and Digital Wallet Platforms
- Stage 3 – Broad Platform and Operating System Integration

#### 7.1.1. Stage 1 – Basic Digital Wallets

Simple applications are already providing some Digital Wallet capabilities. They range from payment wallets like Apple Pay and Google Pay to applications that are highly specialized (e.g. Starbucks App, Air Miles app, grocery chain app). These discrete and basic applications provide the beginning of the Digital Wallet ecosystem.

Such applications will gradually evolve into specialized but diverse solutions where key components of Digital Wallets are separate and distinct – but integrated. Platform providers will step forward and allow application providers to focus on very specialized applications that meet their discrete business needs.

#### 7.1.2. Stage 2 – Specialized Applications and Digital Wallet Platforms

This stage of the evolution of Digital Wallets will be marked by a combination of Specialized Applications that integrate with Digital Wallet Platforms.

- **Digital Wallet Platforms** will provide the capabilities that are commonly needed in a single, semi-consistent software development kit (SDK) or application programming interface (API).
- **Specialized Applications** will leverage the Platform to their and the Digital Wallet owner's benefit. Since the Platform will manage consent, data collection and synchronization, security and more, neither the application developer nor the person needs to worry about those aspects.

We see some early parallels of such an ecosystem in the Personal Data Store space.

For example, Digi.Me provide some Digital Wallet capabilities that allow apps (analogous to Agents) to use data stored in Digi.Me for various purposes. Digi.Me is a Platform that allows People and Organizations to trust that information is under their control, synchronized reliably, shared only under privacy-respecting and consent-basis, and more. Health, financial, social, and many other types of information can be managed on the platform. Specialized Applications can focus on delivering value while the Platform manages things that an application developer would likely not do in a consistent manner. Two example Specialized Applications that focus on leveraging the health records in the PDS are<sup>48</sup>:

- *RetinaRisk* – analyzes health records to determine the risk of Diabetes-related blindness
- *VaxAbroad* – analyzes health records to advise what vaccinations may be required for various parts of the world

The example of Digi.Me provide an excellent analogy of Specialized and Integrated Digital Wallets that will begin to emerge. Arguably some have started. These Specialized and Integrated platforms provide the beginnings of a broader ecosystem. The Digital Wallet space is beginning to see SDKs that provide some of the high-level capabilities that Digital Wallets required (see section [4.3. Detailed Capabilities of Wallets & Agents](#)). It is early days for the Platforms with only basic capabilities being available from the early SDK entrants (e.g. Hyperledger Indy, uPort, and Pillar Wallet).

As the Platforms evolve they will turn into their own markets – until the broader platform (e.g. web browser platforms) and operating system providers step in.

### 7.1.3. Stage 3 – Broad Platform and Operating System Integration

Over time the deep requirements of Digital Wallets will become much clearer. As Stage 2 progresses the broader market will begin to pay more and more attention to the incredible

---

<sup>48</sup> “Digi.Me Applications.” Accessed February 23, 2019. <https://digi.me/share>.

opportunity that exists. Operating system (OS) and broader platform providers (e.g. web browsers, ERP, e-commerce, and more) will begin to bake Digital Wallet capabilities in.

Instead of discrete Wallet libraries (e.g. libIndy<sup>49</sup> from Hyperledger Indy) we will see iOS, Android and even PC operating systems and browsers begin to provide the building blocks required which will lead to ubiquity. Application providers will begin to rely on the OS and broader platforms.

This will cause two key things to happen:

- Application landscape will grow rapidly as other systems quickly integrate OS and broad platform-level capabilities into their applications.
- Digital Wallet Platform providers will begin to disappear – either through mergers and acquisitions or just competition from the OS and broad platform providers that consider Digital Wallets a feature of their products, as opposed to a discrete product line.

## 7.2. Early Business Approaches

The early successes with Digital Wallets will be simple application of the technology to meet very specific use cases. Broad Wallet initiatives at this time are ill-advised. In order to make progress at this early stage, there are two recommended things to consider in building out a Digital Wallet strategy.

### 7.2.1. Single-Purpose Use Cases

Generally applying a Digital Wallet to a single-purpose use case will be the simplest road to success. Examples include:

- Using a Digital Wallet to receive and share a particular Credential that is generally painful when not done using Verifiable Credentials.
  - BC Government's VON, which creates Verifiable Credential versions of corporate registrations, is a starting point. It will evolve to include permits, licences, and other Credentials that anchor back to the corporate registration. Interestingly, and appropriately, BC Government has currently avoided tying a Person to an Organization. This is partially due to the immature nature of applying Delegation via Digital Wallet. Once that issue is better understood they will likely move forward.
- Using a Digital Wallet to meet a very specific use case with multiple parties. Here are some examples:
  - ATB Financial worked with IBM and Workday<sup>50</sup> to prove out an employee onboarding/transfer use case. An employee Credential was issued by IBM through its HR technology partner's system (Workday). That Credential was then

---

<sup>49</sup> <https://github.com/hyperledger/indy-sdk>

<sup>50</sup> [Decentralized Identity: An Alternative to Password-Based Authentication](#)

used to open a bank account. Subsequently that bank account information was provided back to the employer (IBM) for automated salary deposit. The project proved out the utility of sharing high-quality, trusted information to automate processes. Past approaches would have required deep integration with systems and APIs. However, history has shown that even the largest of Organizations can only afford so much formal integration.

- Using in basic form while advanced use cases evolve. There are foundational steps that can be taken in any systems architecture approach. These should be pursued and be aimed at very simple but broad use cases.
  - CULedger is using a basic Verifiable Credential that will be issued by credit unions to provide a common authentication Credential. This Credential, and the process behind it, promises to create a foundational capability that allows credit unions to reassert control of the authentication process. The current authentication processes are fractured and inconsistent with many credit union members needing to manage numerous usernames and passwords. As CULedger evolves there are community Credentials planned but there is understanding required to see exactly how far this goes.
- Using a mini-wallet approach may be useful where a single credential is stored inside an application for later use. This approach can be used to provide a second-factor authentication (2FA) strategy for mobile applications. Instead of a full Digital Wallet, in this case a library is used to embed the capabilities.

The leaders that are pursuing the above example approaches early on are not ignoring where Digital Wallets can take them. Each of the mentioned teams using the single-purpose use cases is using them as building blocks to prepare for their next steps in the space. Focusing on one particular use case allows them to achieve incremental progress that they can build on. They build momentum.

### 7.2.2. Backup & Recovery is Mandatory

Whatever solution is deployed there is a key weakness in all Digital Wallet applications that this study found. None of them have viable backup strategies. While data can be backed up, the processes required are extremely onerous for multiple reasons:

- **Frequency of Backup** – the Digital Wallets change contents regularly, which means the backup files need to be updated. As Digital Wallet use increases these updates could be constant as messages, notifications, and consents are used.
- **Loss of Keys** – the use of mnemonics as seeds to control a Wallet are a beginning step, but asking someone to securely store this seed is not realistic.
- **Complexity** – managing a Digital Wallet at this time is complex, complex enough that very few, your author not included, will safely use Digital Wallets beyond trivial use cases.

### 7.2.3. Simple Trust Hubs

Managing the list of Issuers that you can trust is crucial to early success. If you don't know that a particular Issuer is "official" and/or "trusted" you can't do much with the contents of a Digital Wallet.

Until there are formal standards and approaches to managing the definitive lists of Issuers, any systems being created need to manage the Issuers that are "trusted". At a small scale this is quite manageable but as different bubbles of activity connect, complexity will emerge.

Using a configurable list of Issuers, managed by a repeatable and trusted process will be crucial.

## 7.3. Influence Things

Let's discuss Control versus Influence.

*"Control leads to compliance; autonomy leads to engagement."  
— Daniel H. Pink*

Everybody wants to control the results we get. It is a natural thing to desire – pick an outcome and then achieve it.

There are huge benefits to having control, but control comes with a cost that increases as an exponential. Controlling too much means you end up losing control because the costs of maintaining control overtake the ability to increase control. Cost grows faster than control.

Way faster.

In software 40-80% of total lifetime cost is maintenance (60%), and 60% of maintenance cost is due to enhancements<sup>51</sup>.

Control-freaks want to be able to make certain that things happen in a particular way. Even those of us that have reformed our ways (say it with me: "My name is [your first name] and I am a control freak!")

The problems that stem from that misplaced need for control are manifold:

- **Stifling Growth** – some environments need to be uncontrolled in order to grow. As a community grows the costs of maintaining control create a natural limiter.

---

<sup>51</sup> "Frequently Forgotten Fundamental Facts about Software Engineering", Robert L. Glass, IEEE Software May/June 2001

- **Community Suppression** – when someone places demands on an ecosystem, other members of the community are likely to either stand back to allow them to do things or back away where their ideas conflict.
- **Lack of Resilience** – systems that have rigid control may be strong but they fail when conditions change or when control points are not deeply understood.

*“Leadership is not about a title or a designation. It’s about impact, influence and inspiration. Impact involves getting results, influence is about spreading the passion you have for your work, and you have to inspire teammates and customers.”*

— Robin S. Sharma

Influence is a power function – each of us can influence far more than we can control. The hard part about influence is that it isn’t nearly as predictable as control.

The rewards that come through influence can be incredible.

<p><b>STORY</b> Control vs. Influence Example</p> <p>A quick case to prove the point – Twitter – as an example of the good use of influence and poor use of control.</p> <ul style="list-style-type: none"><li>● <b>Successful Influence</b> – Twitter has exercised limited control while allowing the community to create new features. Retweets (RT) and direct messages emerged from the community – they merely created some tools that helped users do what they already were doing. Arguably where Twitter acts to lightly influence its community it grows.</li><li>● <b>Control Failure</b> – In the early days of Twitter the community was expanding rapidly. Tools and apps were being created and they made Twitter grow faster and faster. Then Twitter exerted control on an ecosystem – and nearly died for it. Twitter was inconsistent and they destroyed successful partners by limiting access and developing competitive features. This failure still impacts the Twitter community many years later. Twitter’s CEO <a href="#">Jack Dorsey apologized in 2015</a><sup>52</sup> and they continue to struggle to rebuild the Twitter developer community.</li></ul>
--

In the Digital Wallet space we need to look at the points of control and influence that are really needed. As you look at the various aspects of a Digital Wallet that you need, ask yourself this

<sup>52</sup> <https://www.theverge.com/2015/10/21/9586084/jack-dorsey-twitter-ceo-apology-developers>

question: “Do we really need the cost of controlling this?” The answer is mostly likely no. Now we need to ask another question: “What can I influence to be as sure as possible we get what we really need?”

The answers there depend on what parts of a Digital Wallet we need. The basic capabilities described in [4.3. Detailed Capabilities of Wallets & Agents](#) and [5. Agents - Deeper Detail](#) are a good starting point. We can influence each of them in many ways:

- Help guide Standards by requesting/insisting that our projects use the evolving standards. Participate where appropriate.
- Create projects that use the open source libraries that are working at the various layers of self-sovereign identity, agents, and Digital Wallets.
- Start working through use cases inside and outside our Organizations and share the learning with the community. Though the intimate details of a project will be confidential, the general patterns will be universal and relatively generic.
- Depending on where we are we can influence in different ways:
  - Government should be setting guidelines for industry to work towards.
  - Companies can begin looking at how things change and which pieces of a Digital Wallet they need now and in the future.
  - Individuals can be contributors on many levels: providing leadership, coding in key projects, and doing the deep thinking needed everywhere.

### 7.4. Help Build the Ecosystem

The Digital Wallet ecosystem is in its early days. The efforts that are underway are just beginning to form what will evolve into a multi-billion dollar ecosystem. We need to understand that early ecosystems like this are a dangerous place to play. For those who are not true innovators or early adopters the best advice is to “wait and see”.

The innovators and early adopters can benefit by starting early. There are three key activities that will ensure success of the ecosystem and of the investment (time, resources, and funds) made in the Digital Wallet space.

Firstly, a focus on activities that help the ecosystem to grow – initially this will be early experimentation and learning. The experimentation and learning will allow key players to build on past successes and avoid failures.

Secondly, the innovators and early adopters who appreciate proper governance will have an outsized impact on the ecosystem. Technology is just one piece of the solution and arguably it becomes commoditized quickly as standards form and functionality becomes common for Digital Wallets.

Lastly, a focus on building relationships amongst different business sectors and even amongst competitors will be crucial. The Digital Wallet ecosystem is going to be enormous – so taking a “piece of the pie” approach won’t work nearly as well as a “grow the pie” strategy.

## 8. The Upcoming Wallet Wars

As a short conclusion we'll discuss the upcoming "Wallet Wars". The ongoing Browser Wars<sup>53</sup> have seen billions of dollars of investment and breaking changes at regular intervals. However, by and large, web browsers work and are mostly interchangeable.

Though, as browsers begin to add Digital Wallet capabilities, the incompatibility and feature mismatch will start to increase again.

The pure Digital Wallet realm is going to go through a similar process - with many players coming into play and vanishing (remember Mosaic? Netscape?)

### 8.1. I Want To Build My Own

There are very few companies that can afford to build a Digital Wallet of their own. Right now the advantage is really on the major mobile operating systems (Apple iOS and Google Android) and the largest of smartphone builders (e.g. Samsung, possibly Huawei or LG).

For now there are a multitude of small startups that are creating Digital Wallet capabilities. The list is enormous but the projects to look at include:

- Sovrin Wallet – the Sovrin Foundation is open-sourcing a Wallet as part of its efforts. It is anchored to the Sovrin Network.
- Evernym – creators of the initial Sovrin Wallet, they have Connect.Me as a (free) commercial offering.
- Pillar – though leaning towards cryptocurrencies it has some interesting features like managing contacts and (notionally) secured chat channels.
- Blockcerts – an early application for managing verifiable Credentials. There are some interesting uses for this app.

For those who want to build their own I recommend re-thinking that idea. Stepping into the space of the Digital Wallet is a very large endeavor. Be certain it is an area that you really need to control. Otherwise push influence instead.



**Darrell O'Donnell** 🇨🇦 @darrello · 29 Oct 2016

Control only what you must. Influence the rest.



---

<sup>53</sup> [https://en.wikipedia.org/wiki/Browser\\_wars](https://en.wikipedia.org/wiki/Browser_wars)

## 8.2. Surviving – Push the Standards

The Wallet Wars are going to take a while to shake out. As different players make moves by introducing new features it will be helpful to monitor where each player is headed. The best way to ensure that your Organization is kept safe is to see which capabilities are most important and push the players to create standards that allow you some portability. Full portability will never be fully realized but you can minimize the pain of moving to a new provider by insisting that basic Standards be supported.

## 8.3. Acknowledgements

First off – big thanks to three of Canada’s leaders in digital identity – each of them has invested incredible effort and funding to support Canada’s burgeoning digital identity leadership:

- **Mike Brown of ATB Financial** for his deep thinking and push to explore the depth and breadth of what a Digital Wallet really is. Over a beer in 2017 I think both of us had a simple view of what has turned into a massive effort.
- **Andrew Johnston of Telus** for his support and pushing on the “don’t reinvent things” input that has bubbled into the broader Digital Wallet and Self-Sovereign Identity space.
- **John Spicer of 2Keys** for his perspectives about what boutique service providers need to understand and what they can offer to the industry. His deep crypto knowledge – from tech to process – is daunting and appreciated.

Thanks go to the leaders at CULedger, John Ainsworth, Rick Cranston, and Julie Esser. CULedger continues to push the credit union forward and its need for Digital Wallet technology is clear. I’ve been proud to serve as CTO to get things aligned for CULedger.

Tim Bouma for many discussions, his deep dive into the current state of the PCTF and how Canada is leading the way in digital identity – especially the key processes that must be protected and assured.

Drummond Reed and Daniel Hardman, both from Evernym and heavy Sovrin community contributors, for their precise terminology and deep thinking that helped create coherence.

Kyle Kemper for many deep dive discussions that went into the cryptocurrency/cypherpunk realm and pulled back to focus on what a Wallet can mean to a person. His book [The Unified Wallet](#) is a great starter to get your brain thinking about where a Wallet can take us.

John Jordan for his consistently deep thinking and challenging questions and his “things and stuff” approach that helps simplify complex topics.

Jason Law, Timothy Ruff, James Monaghan, and Tyler Ruff of Evernym, Inc. for their deep support of Sovrin, efforts at Evernym, and for the open advice that they share with the community. They inherently understand how open Digital Wallets can change the way we do things.

Phil Windley and Nathan George of the Sovrin Foundation for being sounding boards and challengers like Dan Gisolfi (IBM and Sovrin volunteer) for challenging on many fronts about market needs. Many other people in the Sovrin community that are pushing boundaries and

thought: Paul Knowles, “Telegram” Sam Curren, Stephen Curran, Andrew Hughes, Michael Herman, Kyle Den Hartog, Tobias Looker, and many others.

Christopher Allen, and Heather Vescent from the Rebooting Web of Trust realm for their discussions about what a Digital Wallet needs to become.

Julian Ranger and Andrew Carmody of Digi.Me for pushing the boundaries in the PDS space.

And to many others from various organizations: Kim Hamilton-Duffy (Learning Machines), Rouven Heck (uPort/Consensys), Daniel Buchner (Microsoft), Joe Andrieu (Legendary Requirements), Kaliya “Identity Woman” Young (Internet Identity Workshop), Antti “Jogi” Poikola (MyData), Axel Nenker (Deutsche Telekom) and the inimitable pair of Doc & Joyce Searls.