# Digital Credential Wallets

*a white paper from Rebooting the Web of Trust VII*

by Mikerah Quintyne-Collins, Heather Vescent, Darrell O'Donnell, Greg Slepak, Michael Brown, Christoper Allen, and Michael Ruther

**ABSTRACT**

Digital Credential Wallets (DCWs) are becoming more commonplace as more of our physical credentials become digital. In this paper, we provide requirements for digital credential wallet design, offer considerations for key management of DCWs, and go over several real-life use cases.

**INTRODUCTION**

Digital credentials are seeing widespread usage as governments, businesses, and individuals increasingly come online. Users need to be able to store these credentials for ease of use. Moreover, others validating these credentials need to be able to do so in a secure manner. In order to do this, digital credentials are stored in what are called *Digital Credential Wallets* (DCW).

The goal of this paper is to provide an overview of the considerations needed to build digital credential wallets and various use cases to put these considerations into perspective.

### Related Work

There have been a few papers and reports written on the topic of digital credential wallets. These papers can be divided roughly into two categories: exploring uses cases for digital credential wallets and relating digital credential wallets to identity.

In "Cryptocurrency wallets as a form of functional identity" [1], it is argued that cryptocurrency wallets can be seen as a form of functional identity so can be combined with other wallets such as DCW to form the digital analog of a physical wallet. "Who and what is in your wallet" [2] concerns itself with the current state of digital wallets and issues surrounding future usage of digital wallets. "The current and future state of digital wallets" [3] is an extension of the work discussed in "Who and what is in your wallet" [2]; it provides an overview for businesses and governments on the state of digital wallets and goes into detail about every facet of the digital wallet ecosystem.

### Structure of the Paper

The structure of this paper is as follows: first, we provide several definitions of widely used terms, followed by requirements of digital credential wallets. Second, we provide an overview of the key challenges of key management of digital credential wallets. Third, we provide various use cases for digital credential wallets. Finally, we present and suggest various areas for deeper work and investigation in the area of digital credential wallets.

## DEFINITIONS

Before diving into requirements of digital credential wallets, we provide several definitions of well-known terms:

*Definition 1*: A Digital Credential is the digital equivalent of a real-world credential. For example, a digital signature, just like a written signature, attests to the autenticity of a document.

*Definition 2*: A Digital Credential Wallet (DCW) is a either a piece of software or a hardware device in charge of storing digital credentials. For example, the Apple Wallet is a mobile application that stores credit card credentials.

## DIGITAL CREDENTIAL WALLET REQUIREMENTS

We identify several main requirements for a digital credential wallet. These may change whether it is a consumer wallet, an enterprise wallet, or a wallet for a Non-Person Entity (NPE) such as a vehicle, smart object, or dumb object.

### Basic Wallet Requirements

There are 2 basic requirements that all DCWs should satisfy: - Receive and securely store digital credentials, including the ability to both request a credential and be offered a credential - Ability to selectively disclose

credentials to minimize disclosure of information

We go into details about both of these requirements in the following sections.

*Requesting and Storing Digital Credentials.*

Many will argue that a wallet is merely a storage and retrieval mechanism: it handles the cryptographic keys and the encryption/decryption of the "things" that are stored in the wallet. However, that view ignores how those credential get put into a wallet, how they are updated and deleted, and how they are shared with the outside world.

Getting a credential into a wallet requires multiple approaches: - Alice offers to send Bob a Credential; OR - Bob requests a Credential from Alice.

Once that initial offer/request is completed the following happens: - The Credential is generated. - Alice then sends the Credential to Bob: one that is uniquely controlled by Alice (or her designated Agent).

*Selective Disclosure*

The classic case of using a particular credential for multiple purposes can explain the utility of *Selective Disclosure*. Using a digital driver license one can easily imaging the following unique presentations of the credential: - Full Disclosure: present a full driver license 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".

Note that 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" card. That's a different department/ministry.

## KEY MANAGEMENT CONSIDERATIONS FOR DIGITAL CREDENTIAL WALLETS

Digital Credential Wallets (DCWs) are used for *storing* credentials, not issuing them. However, there are circumstances when they may need to manage public/private keypairs. This section will first describe one such scenario, and then will go over methods for recovering from key loss (since that is always a concern when public-private keys are used).

### Example: Using Keys As A Second Factor Authentication Method

Airport security checkpoints often ask visitors for their ID, typically a driver's license, as an example of a government-issued identity credential.

Our DCW could simply store a digitially-signed driver's license and beam that information to the security guard

as proof of ID. While this could be sufficient proof of identity in some scenarios, there is one issue with this example, and that is that the ID could have been stolen. It would be nice if there were some additional, second factor, showing that the information on the ID is indeed valid and belongs to the current credential holder in question.

When a person is asked for ID in the United States, they usually present a driver's license. How does the person asking for ID (the verifier), verify that the driver's license is both *authentic* and actually *belongs* to the holder?

To verify the ID is *authentic*, they verify that the ID has certain markings (for example, holograms and microprint) that are costly to forge.

To verify the ID *belongs* to the holder, they check that the photo on the ID matches the face of the holder and might also quiz the holder on some of the data present on the ID (for example, their birthdate).

A DCW has the ability to improve upon this process by replacing the hard-to-forge physical identity card with a hard-to-steal digital secret called a *private key*. The wallet may still combine this secret with a digital photograph of the holder (signed using the private key) to fully replicate security properties of physical IDs. Note that the photograph does not need to be stored online, it just needs to be signed by the private key of the issuer.

So it seems that holder keys are only relevant when the holder goes to an issuer to receive their ID credential, in order to prove to the issuer that they are the owner of a DID.

**Recovering from Key Loss**

The DPKI overview document [4] describes various ways in which one can recover from key loss. All of the methods presented make heavy usage of *social key recovery*, a key recovery process in which pieces or shares of private keys are stored with trusted parties such as family and friends. Keys are divided into pieces using *Shamir secret sharing* and *threshold cryptography* [5].

When setting up their DCW, one creates N shards of their private key, using the method of their choice, and distributes these shards to trusted parties. Depending on the parameters of the method used, one only needs to retrieve M of these N shards in order to recreate the private key. Note, however, that this does not help in the case of key compromise. For more details in the case of key compromise, see section 6.2.2 in the DPKI overview [4].

## APPLICATIONS AND USE CASES

In previous sections, we have outlined the requirements and key considerations to take into account when building and handling digital credential wallets. In this section, we aim to present how all of these components come together in practical use cases.

**Account Opening**

When opening an account with a new organization (e.g. telco, utility, bank) that organization requires an individual to provide certain information. This can be provided through the completion of various forms (online or paper) and then proof of some of the details (e.g. presentation of driver license). Through the use of a digital credential wallet, it would be possible for the organization to request all of the data from that wallet, and for the wallet to then provide the details back, if they are present in the wallet.

In the scenario of opening an account online, the following steps could take place: - The consumer visits the business' website and requests to open an account - The website indicates that the consumer can complete the various forms and provide proof of government ID (e.g. through selfie and photo of driver license) or they could choose to use their digital credential wallet - If a consumer chooses to use their digital credential wallet, the site indicates the information that it requires such as government issued ID, proof of other business (e.g. bank, utility) relationships, proof of employment - By establishing a connection between the site and the digital credential wallet, often through QR code or SMS, the request for credentials is made - Using the digital credential wallet, the consumer confirms the information that it would like to share, which may include selecting specific credentials (e.g. driver license vs passport, or prior bank relationship vs telco relationship) - The wallet shares the verified credentials with the website - Depending on the protocol, the website verifies the validity of the presented credentials

**Employee Onboarding**

Not too dissimilar to the Account Opening use case, employee onboarding requires an employee to present forms of various credentials in order to begin employment. Depending on the type of job, the credentials required may include: - government issued ID - SSN/SIN - education - training - professional designations - prior employment - direct deposit bank account

Some of the above could be provided during the applications process (e.g. prior employment, educations), while some are only relevant once the employee is being hired.

A possible scenario for this use case could be:

- An employee accepts an offer and then receives a confirmation email, which contains a link to a web page with the employment agreement and a request for credentials
- The web page could include a QR code that contains a request for the necessary credentials from a digital credential wallet
- Once scanned with the wallet, the wallet displays a list of what the company is requesting and the employee confirms what details it will provide and from which sources

The credentials are then shared between the wallet and the organization for their storage

**NPE: Non Person Entitity**

NPE is a non-person based entity; it is a term to describe a non-human object that has an identity. It may be a smart object with specific technical functionality (like collecting or sharing data, e.g. a weather station) or it may be a dumb object that does not integrate with technology for sharing information. These objects need their own wallets to collect and share credentials.

Another use case class is the introduction of Digital Credential Wallets for objects or machines. This will enable us to overcome some of the virulent issues in today's global industry like provenance, authenticity, tracking, proof of audit trails, and compliance. Creation of Digital Credential Wallets are hereby a key requirement for so-called digital twins of objects, machines, or IoT devices, where digital twins are a digital representations of such objects that store lifecycle data and events, including assembly, testing, transport, operations, and decommission.

*Motorcycle Wallet: A Complex Object*

A motorcycle has a wallet that keeps digitally native credentials. These credentials are given by various entities. The wallet needs to be accessed by the owner of the motorcycle. There may be situations where data from the wallet should be shared. This is a complex object because it is both "smart" and "dumb."

The wallet needs to hold different kinds of credentials from different entities, such as human entities, corporate entities, service providers, and governments, as well as data from the vehicle itself. This data may need to be accessed by a variety of different entities as well, including humans identities, corporations, governments, and service providers. The wallet needs to address delegation and access transfer in the context of changing ownership of the object itself: a motorcycle.

## CONCLUSION AND FUTURE WORK

In summary, we have presented requirements for digital credential wallets, key management considerations for such wallets, and use cases. Moreover, we have presented definitions of terms that are used colloquially in the self-sovereign identity space so as to facilitate collaboration without ambiguity.

There are various areas of future work in the area of digital credential wallets. As this is a growing field, we only present a few areas of future consideration. First, improving the user experience of digital credential wallets is multifaceted and involves many components. Easy to use interfaces are paramount to making digital credential wallets widespread. Second, even though we have presented core considerations for key management in digital credential wallets, there is a wide design space in which to make it easier for both digital credential wallet users and builders to manage and handle private keys. Last but not least, further research into privacy considerations for DCWs is an important area to look into due to both increasing awareness in the public and regulations from governments. This was a non-exhaustive overview of possible areas of research in the field of digital credential wallets.

**REFERENCES**


1. Quintyne-Collins M, Mehar A (2018). Cryptocurrency wallets as a form of functional identity. Topics and Advanced Readings for the Rebooting the Web of Trust 7 Workshop. https://github.com/WebOfTrustInfo/rwot7-toronto/blob/master/topics-and-advance-readings/Cryptocurrency%20wallets%20a%20an%20application%20of%20Functional%20Identity.md
2. O'Donnell, Darrell (2018). Who and what is in your wallet. Topics and Adcanved Readings for the Rebooting the Web of Trust 7 Workshop. https://github.com/WebOfTrustInfo/rwot7-toronto/blob/master/topics-and-advance-readings/what-and-who-is-in-your-wallet.md
3. O'Donnell, Darrell (2019). The current and future state of digital wallets. Independently published
4. Allen C, Brock A, Buterin V, Callas J, Dorje D, Lundkvist C, Kravchenko P, Nelson J, Reed D, Sabadello M, Slepak G, Thord N, Wood H.T (2015). Decentralized Public Key Infrastructure. Rebooting the Web of Trust 1 Workshop. https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf
5. Shamir, Adi (1979). "How to share a secret". Communications of the ACM. 22 (11): 612–613. doi:10.1145/359168.359176. https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf
6. Rait, Seth (2016). "Shamir Secret Sharing and Threshold Cryptography" https://sethrait.com/Shamir-Secret-Sharing-and-Threshold-Cryptography
7. Blakley, G.R. (1979). "Safeguarding Cryptographic Keys". Managing Requirements Knowledge, International Workshop on (AFIPS). 48: 313–317. doi:10.1109-/AFIPS.1979.98. https://pdfs.semanticscholar.org/32d2/1ccc21a807627fcb21ea829d1acdab23be12.pdf
8. Smith S.M, Gupta V (2018) Decentralized Autonomic Data and the three R's of key management. Rebooting the Web of Trust 6 Workshop. https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/DecentralizedAutonomicData.pdf
9. Reed D, Chasen L (2016).Requirements for DIDs (Decentralized Identifiers). Rebooting the Web of Trust 2 Workshop. https://github.com/WebOfTrustInfo/rwot2-id2020/blob/master/final-documents/requirements-for-dids.pdf
10. Sporny, Manu (2018). A Verifiable Credentials Primer. Topics and Advanced Reasings for the Rebooting the Web of Trust 7 Workshop. https://github.com/WebOfTrustInfo/rwot7-toronto/blob/master/topics-and-advance-readings/verifiable-credentials-primer.md


---

**ADDITIONAL CREDITS**


**Lead Author:** Mikerah Quintyne-Collins

**Authors:** Heather Vescent, Darrell O'Donnell, Greg Slepak, Michael Brown, Christoper Allen, and Michael Ruther


---

**About Rebooting the Web of Trust**

*This paper was produced as part of the Rebooting the Web of Trust VII design workshop. On September 26th*

*through 28th, 2018, over 40 tech visionaries came together in Mississauga, Ontario to talk about the future of decentralized trust on the internet with the goal of writing 3-5 white papers and specs. This is one of them.*

**Leadership Team:** Christopher Allen, Joe Andrieu, Kim Hamilton Duffy, Manu Sporny, and Heather Vescent

**Gold Sponsors:** Civic, Protocol Labs, Sovrin, an anonymous donor

**Silver Sponsors:** HTC, Microsoft, PTB Ventures, Spherity, Tierion

**Community Sponsors:** Blockchain Commons, Learning Machine, Legendary Requirements, Purple Tornado, Veres One

**Workshop Credits:** Christopher Allen (Founder), Joe Andrieu (Producer and Facilitator), Shannon Appelcline (Editor-in-chief), and Claire Rumore (Graphical Recorder)

*Thanks to our other contributors and sponsors!*

**What's Next?**

The design workshop and this paper are just starting points for Rebooting the Web of Trust. If you have any comments, thoughts, or expansions on this paper, please post them to our GitHub issues page:

https://github.com/WebOfTrustInfo/rwot7/issues

The ninth Rebooting the Web of Trust design workshop is scheduled for September, 2019 in Prague, The Czech Republic. If you'd like to be involved or would like to help sponsor the event, email:

rwot-leadership@googlegroups.com

---