The History and Future of Digital Wallets

Stephen Wilson, Las Vegas, 31 May 2023

Principal, Lockstep Consulting

www.lockstep.com.au/DVP

Digital wallets are becoming a part of daily life for many. The verifiable credentials push makes wallets seem like new technology, but the 1990s SIM card is probably the first genuine cryptographic credential. We can trace the history of digital wallets with a Capability-Maturity Model (CMM) from paper and magnetic stripes to chip and mobiles. Fundamentally, these form factors steadily improve the ability to prove the properties of the data carried. Today’s smart phone wallets prove the origin of each credential, possession by its rightful owner, the manufacturer and history of the wallet, and other metadata.

The most important development to come will be wallet management schemes and two-sided business models to make verified data globally accessible and legible.

Digital wallets

Digital wallets are fast becoming a part of daily life:

- ticketing
- payments
- health certificates
- driver licensing
- physical access control

EU eID is coming to Apple and Google wallets.

Where will the “wallet wars” really be fought?

The mobile digital wallet has become a fixture in digital identity. It is even being touted as surpassing the web browser as the primary user interface and user experience of the future internet. It’s early days. Naturally there are various ways to organise and present a user’s collection(s) of digital credentials, in native wallets and mobile apps. There will be a contest of ideas around preferred UX. But the suggestion of a *wallet war* misses the most critical success factor for utility and interoperability, and it’s not at the wallet level!

CyberForge ABOUT JOURNAL

Asymmetric wallet wars

By ANIL JOHN on 15 December, 2022 | Permalink

The user, the identity provider, the relying party all have different power dynamics

~ Kim Cameron

CyberForge.com

‘Digital wallets to be as essential as browsers’: OpenWallet Foundation calls for builders

Feb 24, 2023, 6:38 pm EST | Frank Hersey

CATEGORIES Biometrics News | Civil / National ID | Features and Interviews

≡ Forbes

FORBES > MONEY > FINTECH

The Wallet Wars Are Not About Money, They Are About Identity

David G.W. Birch

Contributor ⓘ

Author, advisor and global commentator on digital...

Follow

“Interoperability”

In response to the prospect of vendors monopolising digital wallets, the Open Wallet initiative was founded last year (at Identiverse 2022 in fact). The project has since found a home at the Linux Foundation.

The OWF aims to specify “an open source wallet engine that promotes interoperability around the world”.

But the question of interoperability is not confined to the wallet.

Open-source principles and the fight against vendor lock-in are laudable, but these are not sufficient to ensure interoperability of verifiable credentials.

In partnership with:

THE LINUX FOUNDATION Research

Why the World Needs an Open Source Digital Wallet Right Now

February 2023

The evolution of digital wallets 2003–04

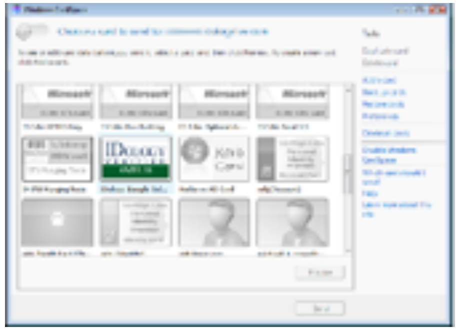
The history of digital wallets, especially as secure data carriers, helps to unpack *interoperability*.

Some of the earliest general-purpose wallets were the multi-function national smartcards of Hong Kong (iLife, 2003) and Malaysia (MyKad, 2004). These supported government ID, driver license, border control, access to health records, transport ticketing, and banking.

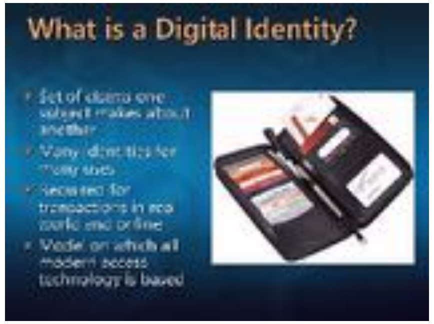
An international standard for identification cards emerged, ISO/IEC 24727, focused on supporting multiple applications and a trio of functions known as "IAS" or *Identity, Authentication & Signature*. (Incidentally, it's a huge shame that *signature* fell by the wayside, for data signing turns out to be critical to data protection).

In general-purpose computing, interest grew in having a choice of digital credentials. In 2005, Kim Cameron launched *The Laws of Identity* which led to Infocards*,* Windows CardSpace (2007), and the open-source Project Higgins. It also popularised the wallet metaphor.

Picture credit: Doc Searls



Mike Jones, *Self Issued*, 2008



What is a Digital Identity?

- Set of claims one subject makes about another
- Many identities for many uses
- Required for transactions in real world and online
- Model on which all modern access technology is based

"Cardspace". March 2007

The smartest move 2011–12

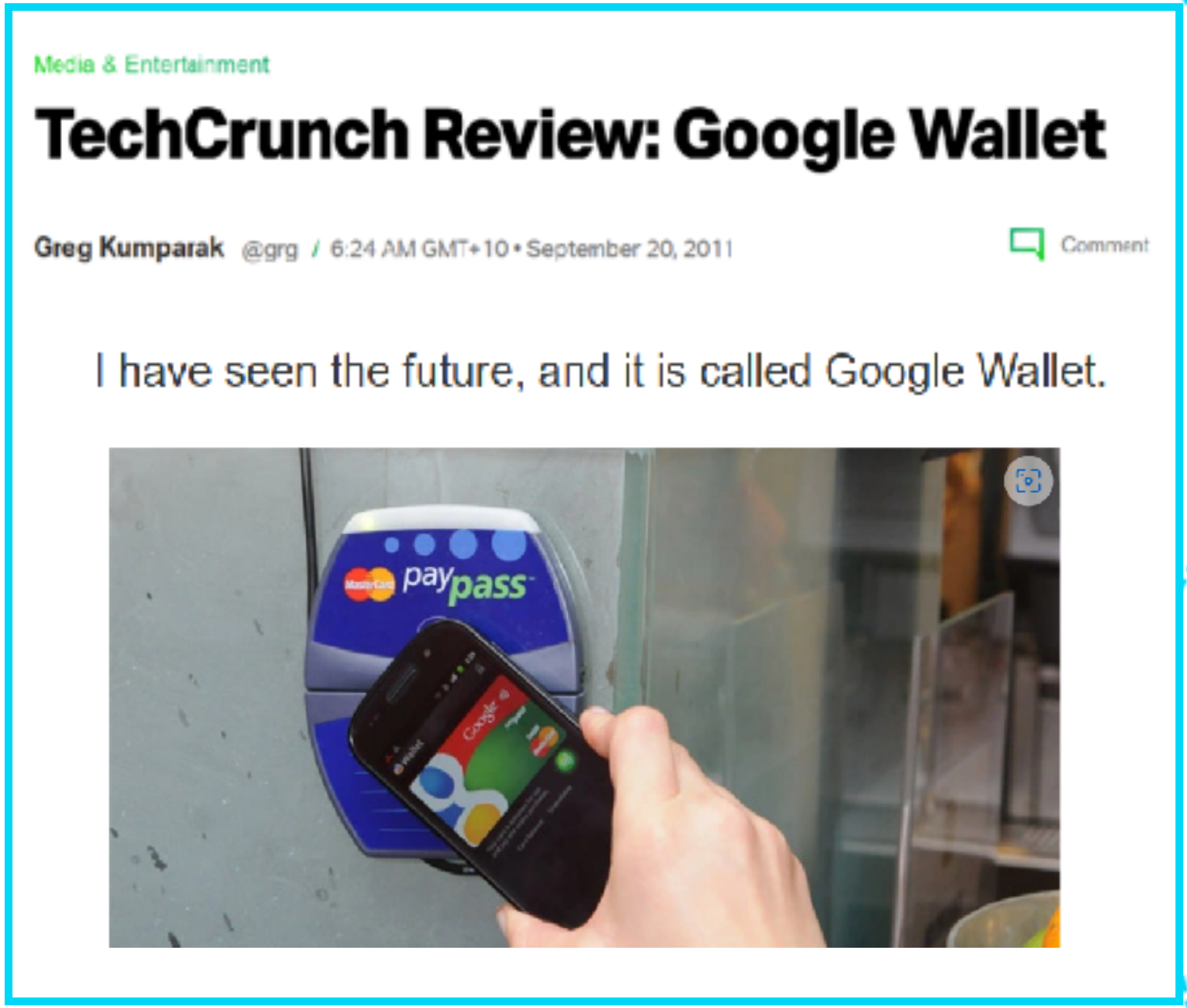
After just four years, Microsoft pulled support for CardSpace. Infocards were such a good idea, but their market failure remains largely unexamined by the industry. Same with the well-funded but ultimately doomed NSTIC and GOV.UK Verify.

The year 2011 proved to be a watershed for “Identity 2.0”. The roll-your-own single sign-on OpenID movement collapsed (and yet the OpenID Connect OIDC protocol survived and is now firmly part of the landscape).

But then the smartphone wallet was launched, and personally controlled digital credentials have since been unstoppable.

Google Wallet featured NFC radio-frequency presentation of payment details, replicating the payWave UX.

In 2012, Apple followed with Passbook in iOS 6, featuring coupons, tickets, and boarding passes. Passbook at first lagged behind Google Wallet, with no NFC interface and no payments.



Media & Entertainment

TechCrunch Review: Google Wallet

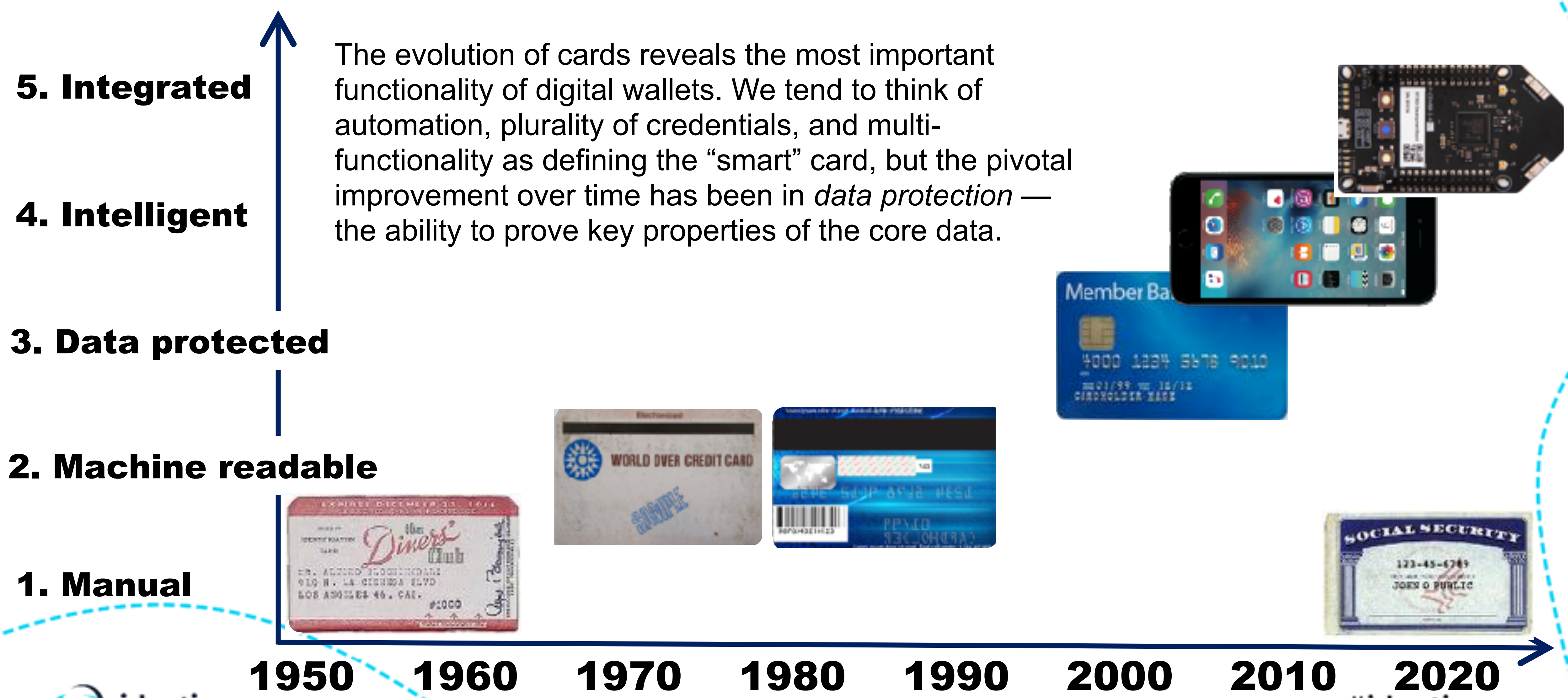
Greg Kumparak @grg / 6:24 AM GMT+10 • September 20, 2011

Comment

I have seen the future, and it is called Google Wallet.

Evolution of payment and identification cards

The evolution of cards reveals the most important functionality of digital wallets. We tend to think of automation, plurality of credentials, and multi-functionality as defining the “smart” card, but the pivotal improvement over time has been in *data protection* — the ability to prove key properties of the core data.



5. Integrated

4. Intelligent

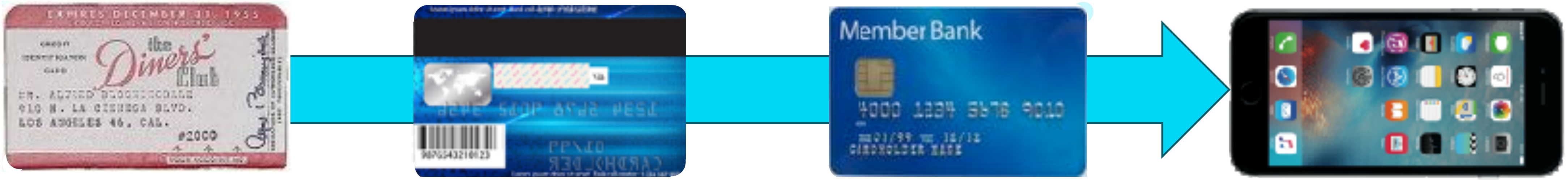
3. Data protected

2. Machine readable

1. Manual

1950 1960 1970 1980 1990 2000 2010 2020

Claims and proofs, data and metadata



The ability to prove key properties of core data leads to a broader view of data protection, beyond privacy (in GDPR's sense of data privacy) and beyond cybersecurity's traditional confidentiality, integrity and availability (CIA). We can protect the properties that make data reliable, useful, fit for purpose, and valuable.

Think about the importance of *evidence*. When facts are in dispute, what makes them reliable is evidence. The Self-sovereign Identity movement has normalised the concepts of claims and proofs. This all boils down to data and metadata.

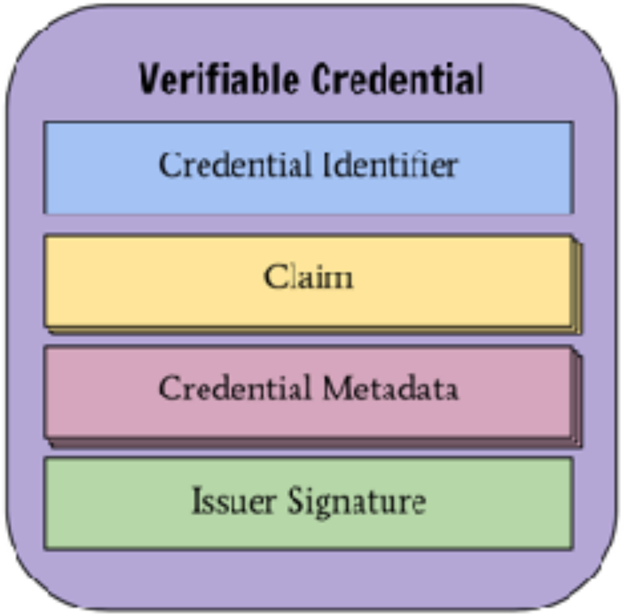
Payment cards have always carried a primary account numbers (PAN). As new types of fraud emerged, the system rolled out improved ways of protecting the PANs against misuse or counterfeiting. Over many decades, there's been no essential change to the idea of PANs, nor the cardholder agreements, nor the merchant business rules.

The PAN carried in a smart wallet is exactly the same as that on a mag stripe card – but it is a *better* PAN! We know it can't have been skimmed and replayed by an imposter.

The core data is made better by metadata, including digital signatures which prove where the data originated, and prove it was presented by the rightful cardholder.

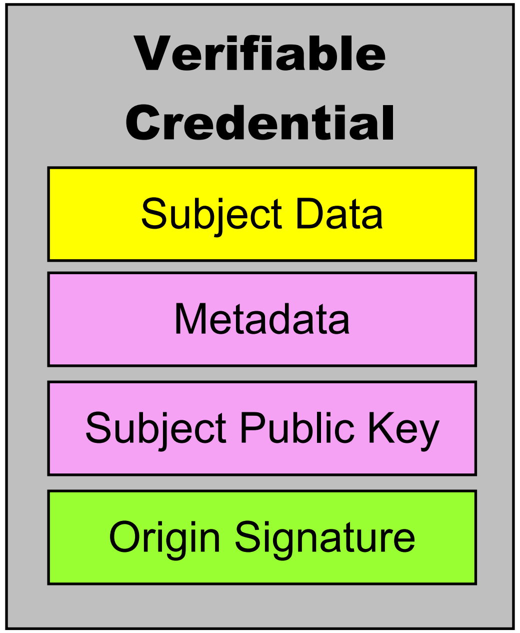
The essence of verifiable credentials

Let’s now look at the generic architecture of a digital wallet and how these things are going to scale into the future. We start with the modern verifiable credential (VC), according to the W3C model, and abstract the essential elements.



W3C Verifiable Credentials Data Model 1.0, 2022

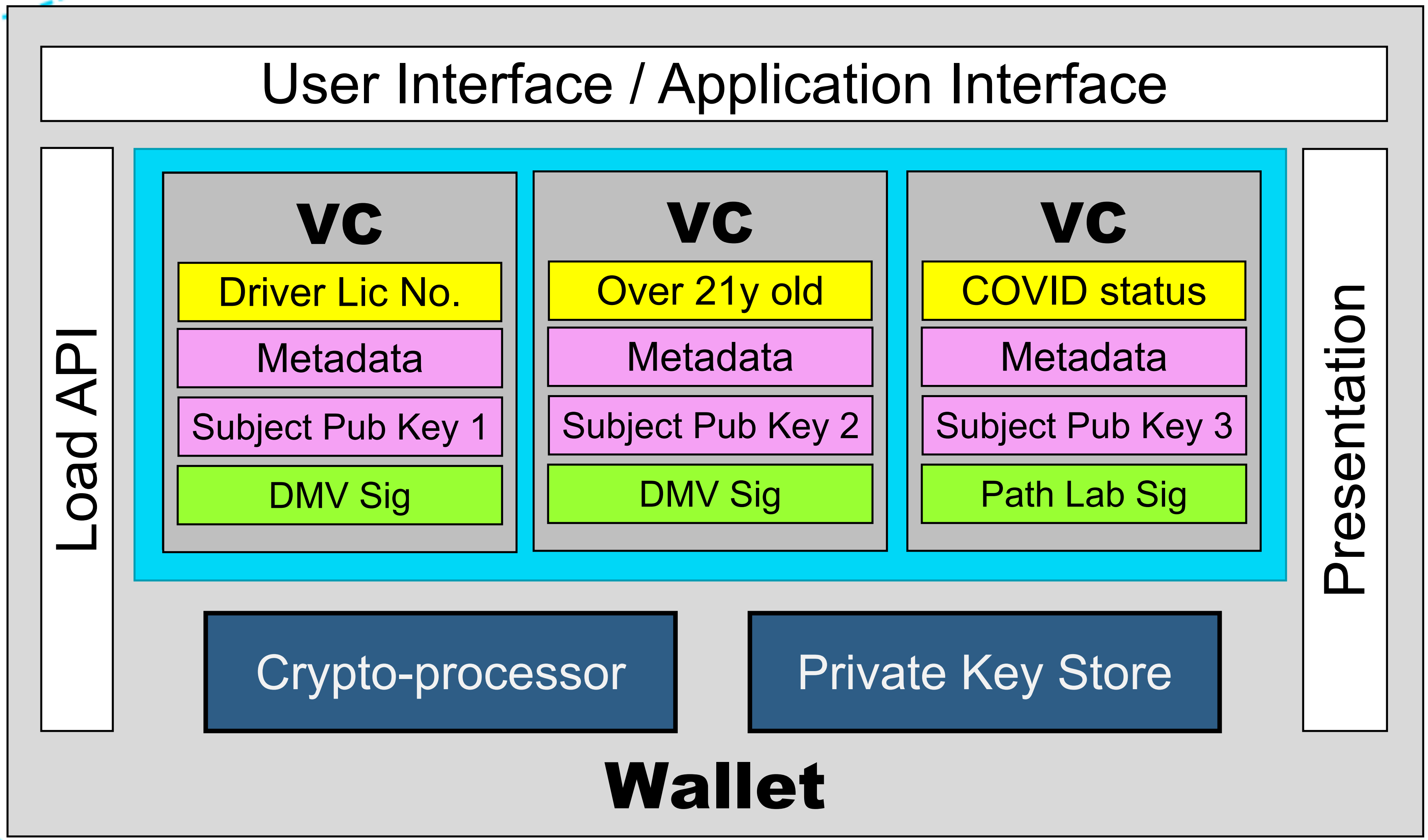
A VC contains data about an entity, vouched for by a recognised authority. The entity is the *subject* of the credential, classically a person, often regarded naturally as the *holder*. There is additional metadata to help guide how others use the VC, such as issue date, expiry date and, most importantly, details about (or pointers to) the terms and conditions under which the VC was issued. The issuer digitally signs the VC to prove its origin.



Copyright Lockstep Consulting 2022

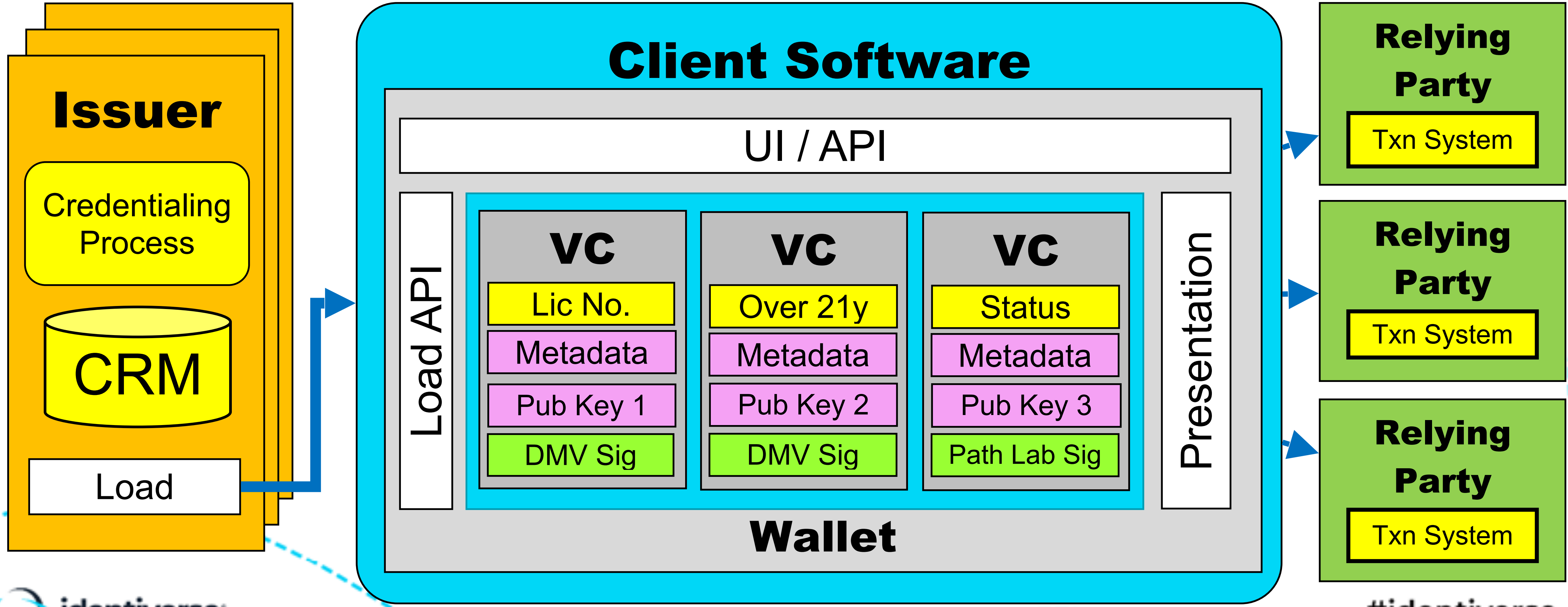
The most powerful VCs also bind a key-pair of the credential holder, so they can digitally sign each presentation of the credential, to prove possession and to impart their relevant authorisation on their transactions. The world’s first true cryptographically verifiable credential was arguably the SIM card. The SIM contains your international cell phone account ID, signed by your mobile phone company. Every phone call session is digitally signed at the start and end, binding your account details to your call, to allow accurate billing.

Wallet


User Interface / Application Interface
Load API
VC
Driver Lic No.
Metadata
Subject Pub Key 1
DMV Sig
VC
Over 21y old
Metadata
Subject Pub Key 2
DMV Sig
VC
COVID status
Metadata
Subject Pub Key 3
Path Lab Sig
Presentation
Crypto-processor
Private Key Store
Wallet

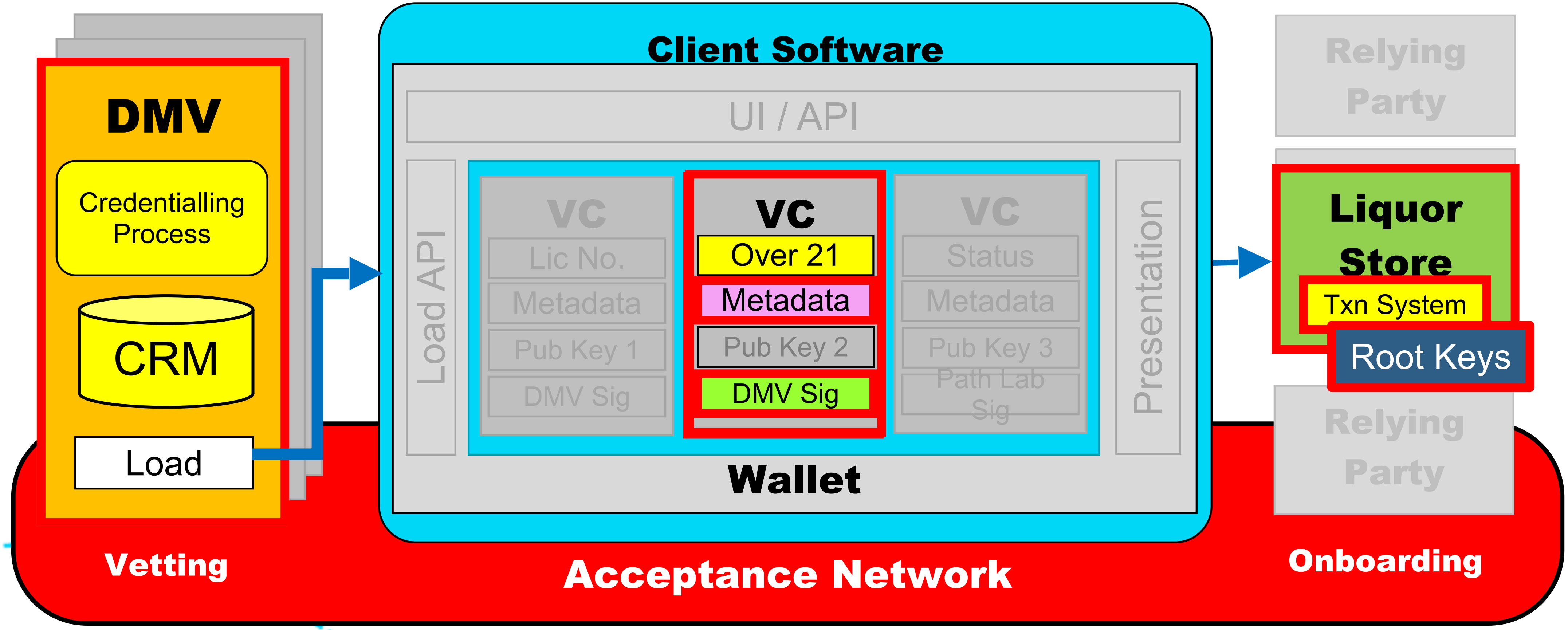
Wallet in context

The wallet is merely a container for credentials, each of which operates in its own context beyond the wallet. The context is set by the *relying party* (or more usually on their behalf by an industry group). And credentials are only relevant in specific transaction systems. RPs will not accept any old credential or issuer — because the RP wears the consequences of the credential being wrong. RPs each have their own criteria, often subject to regulations, for which credentials are fit for purpose.



Verifiable credentials don't verify themselves

If the customer doesn't have a credential of the right sort, the relying party *as risk owner* does not have to accept it. It's the same with everyday credentials like charge cards: If you want to use a Diners Club card at a store but it only takes Mastercard or Visa, tough luck. Note that *the RP must make arrangements in advance for the types of credentials they are willing to* accept. There is never any real-time negotiation to present an unexpected type of credential. And the RP needs to have their transaction system configured with the right root keys to verify signatures on credentials and presentations. *These arrangements can only be made at scale through a network*.



The uncomfortable truth about verifiable credentials

"The whole system of identity emanates from the relying parties …

If they don't like it, it goes nowhere" — Kim Cameron, IIW 2016, quoted by Tarun Wadhwa

The truth was spoken by none other than the late great Kim Cameron a few years ago at IIW.

Relying parties call the shots. It doesn‘t matter what credentials you carry, nor what wallet technology you use; if you're not presenting credentials that the RP reckons are fit for purpose, they will not be accepted.

This is asymmetry is not about identity. It's about risk, the party that carries the most risk, and their right to manage the risk as they see fit.

Photo: Doc Searls

Credentials need networks

In conclusion, let's return to the credit card. A credit card is only legible when a merchant has made prior arrangements to ingest and process it. The merchant can't do anything with a card unless they have the right equipment and moreover *the right contract in place* with a network.

Look under the covers at what "We accept Mastercard" means. The merchant has decided what credentials are fit for purpose. They have acceptance mechanisms in place including liability arrangements, with baked-in expectations of which credentials are going to meet their needs. That's their prerogative as *risk owner*. You can use any card you like — as long as the merchant accepts it.

The superpower of the network is it allows you to use a credit card anywhere on the planet without the merchant knowing you, but more significantly, without knowing your bank, the issuer of that card.

It's going to be the same reality with verifiable credentials. No relying party will know what to do with a VC unless they have an arrangement in place. But we can't have bilateral arrangements between every RP and every issuer. VCs and wallets need acceptance networks which scale globally, just like the credit card networks scale.

That's the focus of Lockstep R&D — a model data verification network. www.lockstep.com.au/DVP.