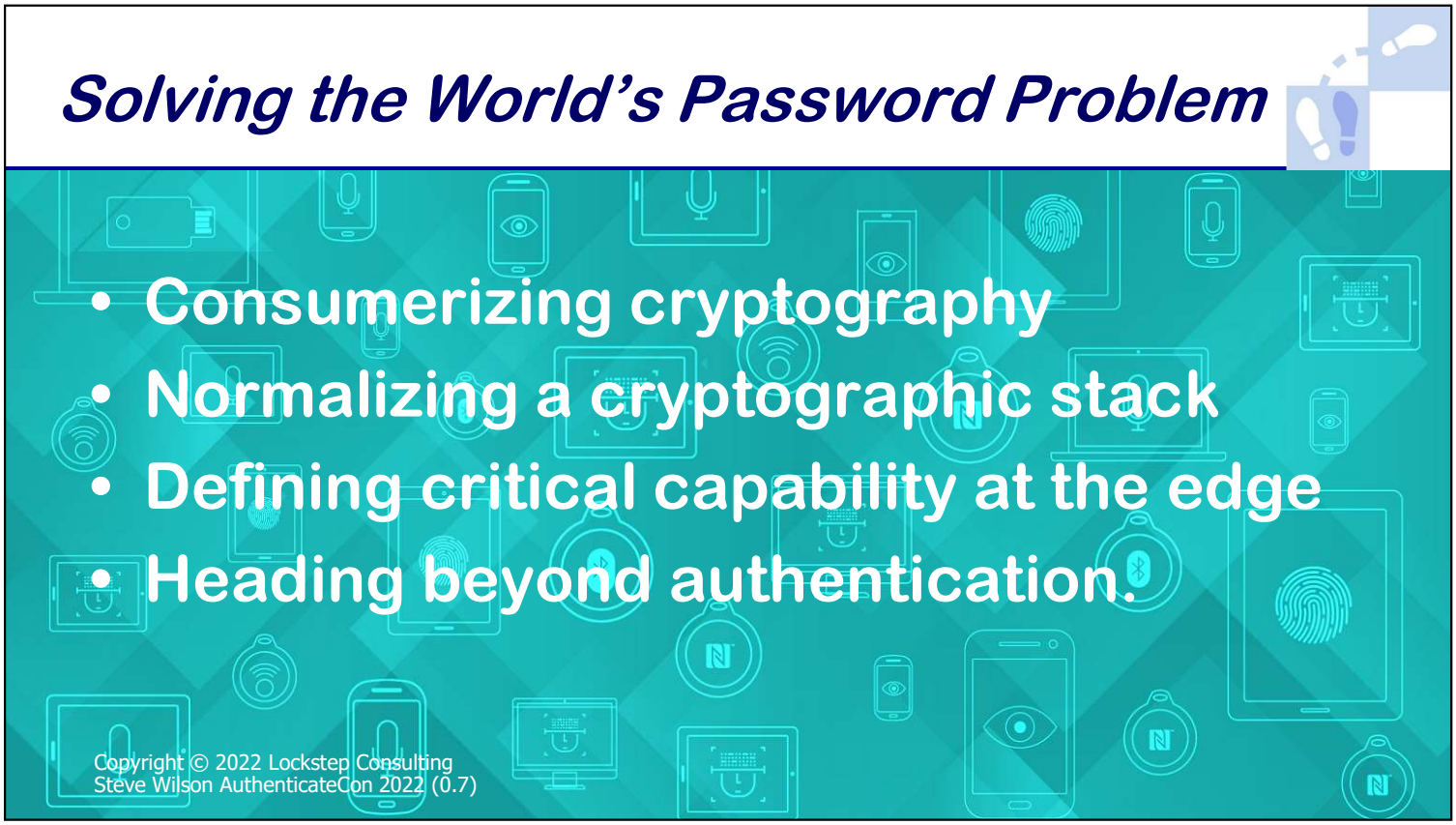
I have a vision about the future of FIDO in the digital ecosystem as our expectations for data protection evolve. We recognise data now as a utility, as important as clean drinking water or stable electricity. FIDO has played a crucial role in normalising cryptography, establishing a quasi-standard technology stack that extends from the cloud all the way out to the edge.

I rate the FIDO Alliance as the most important identity industry consortium of all time. It has established the building blocks of what is turning into a critical two-sided market for authentication and data quality.

I'm going to show you today how we can extend those building blocks from authentication of individuals and their devices through to the authenticity of all things, thus protecting data as a utility in the new economy.



FIDO's mission was always to solve the world's password problem. Its founders sought to leverage the powerful hardware-based cryptography that was becoming increasingly common in the mid 20-teens.

Along the way, FIDO has helped to *consumerize cryptography*, establishing a commonplace cryptographic technology stack in edge devices. The de facto standard now includes secure elements, key generation and data signing on the device, and biometric matching on the device.

FIDO is adjacent to many of today's most impactful computing developments; because FIDO technology is the cousin of portable cryptography technologies that go back to over 30 years ago.

These capabilities can now lead us beyond authentication to a bigger, more urgent challenge.

FIDO's cousins

"Leading at the Edge: FIDO and the Normalization of Cryptography" – AuthenticateCon 2022
Steve Wilson AuthenticateCon 2022 (0.7) Copyright © Lockstep Consulting 2022

The FIDO Alliance was borne of an emerging world of sophisticated hardware-based cryptography, which also enabled the defining consumer security developments of our time:

- verifiable credentials
- cryptocurrency, and
- personal mobile data wallets.

FIDO protocols are the state-of-the-art expression of best practices and standards that have been converging over roughly three decades. In the 1990s, strong cryptography was confined to defence applications. As the cost of cryptographically capable microcontrollers fell, strong authentication and data signing became embedded in certain smartcards and e-passports. The smart phone with in-built secure elements made "defence grade" security available to everyone, and moreover, completely seamless thanks to well-engineered biometrics.

1. U.S. government Fortezza card with 1024 bit RSA and other classified features c.1999.
2. French national health insurance *Sesam Vitale* smartcard with digital signature capability.
3. New Queensland Driver Licence (AU) had a chip, originally planned to support e-govt 2010.
4. Rainbow iKey "reader-less smartcard" with PKI capabilities c. 2000
5. U.S. federal government PIV-I card 2014
6. ICAO-standard e-passport.
7. Trusted Platform Module (TPM) chip.
8. Yubikey "security key" FIDO authenticator.
9. Trezor dedicated hardware cryptocurrency wallet.
10. Apple iPhone and Apple Watch digital wallets.
11. Microsoft Azure Sphere IoT microcontroller.

The right place and time

2003

2012

FIDO's founders saw the potential for embedded cryptography to be so streamlined users would be unaware of it. FIDO born in 2012 as mobile devices were growing in sophistication and availability, and public key technologies we being automated.

The world had public key smartcards for twenty years to that point. The French Sesam Vitale health card was in use from the early 1990s. In 2003, Bill Gates committed Microsoft to smartcard authentication, forecasting that "Over time we expect most businesses will go to smart card ID" (ref: Bill Gates' Executive E-Mail c. 2003.

But difficulties with smartcard readers inhibited adoption.

With the advent of the smart phone, consumers were coming to possess high-grade cryptography (whether they knew it or not).

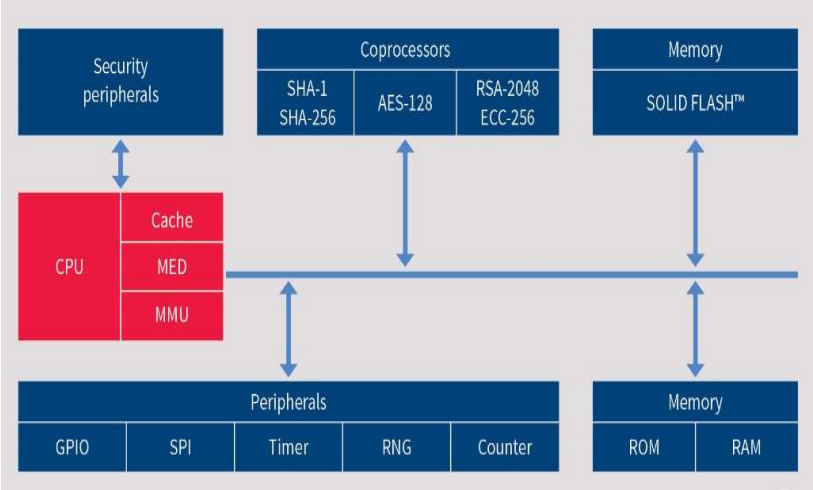
Famously, it is said that the smart phone today has more computing power within it than all of NASA did at the time of the Apollo moon landings.

Even more remarkable perhaps for security is that the smart phone has more cryptographic processing power than the National Security Agency had at its disposal in 1999.

Picture credit:
https://en.wikipedia.org/wiki/File:MOCR_2_Building_30_JSC_angle_view.jpg; licensed under the Creative Commons Attribution-ShareAlike 4.0 License.

A cryptography stack

- **Key generation**
- **True random number generator (TRNG)**
- **Private key enclave**
- **Digital signatures**
- **Hardware roots of trust.**



Source: Infineon Inc.

FIDO in effect has consumerized cryptography.

And it has normalized, almost standardized, a cryptography stack; that is, a minimum commonplace suite of functions.

Developers, architects and *policy makers* can now pretty well rely on these core cryptographic primitives being available in consumer devices.

Properties of the cryptography stack

The state-of-the-art mobile processors are compact, with relatively small pieces of software, and relatively easy to certify.

They are personally protected by biometrics or PIN (matched on device, one-to-one).

More subtly, these personal devices have become *habituated*. They are on our person almost all the time. We feel viscerally how important they are, so safekeeping is becoming second nature. We know to lock our phones just as we lock our cars.

So not only can technologists now assume that a common cryptography stack is available on which to build apps; *they can also assume that almost all users are operating that stack safely.*

Of course, the technology is not perfect, but think about the tacit assumption behind smartphone payment cards and airline boarding passes: these are capabilities of enormous consequence which must be almost guaranteed to be in the right hands. So, we already have system-wide assumptions that virtual credentials have been provisioned to the right users, and they remain under the control of those users and no one else.

What's a cryptography stack *for*?

The cryptography stack allows for digital actions to be bound to human users because those users are closely associated with their devices and the keys contained within.

Binding devices to users

- The all-important private key never leaves the user's control.
- An artifact verified as being signed by that private key can be assumed to have come from the device and hence the user.

Strong authentication

- "Phone as second factor" one of the preferred MFA modes now.
- People tend not to lose control of their phones; strong behaviours protect the phone.

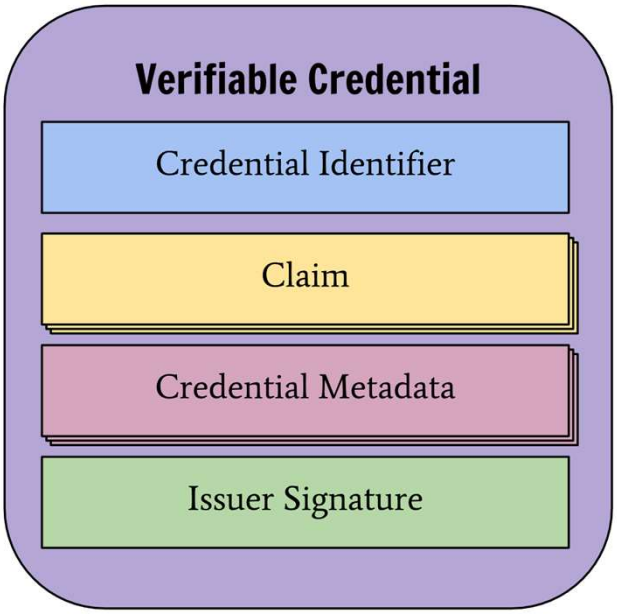
Registering devices -- and hence users

- A registered device like a cell phone comes to be in the user's possession only after a strict protocol (i.e. ceremony).
- Loading additional private keys and credentials to the wallet can be subject to *separate* protocols or ceremonies.
- Artifacts signed by private keys in the phone *memorialise* these ceremonies.

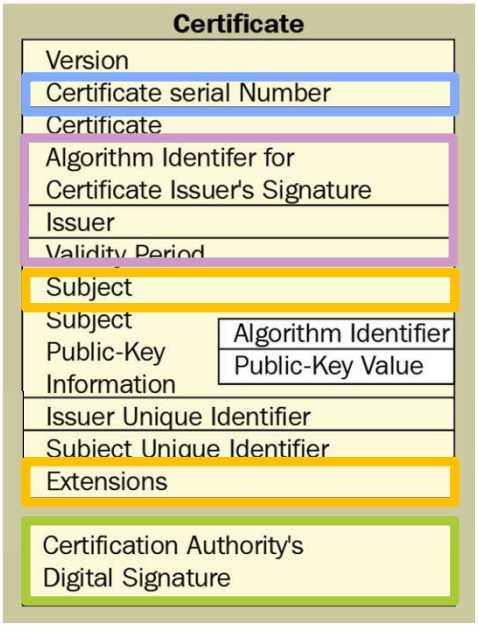
Proof of possession

- A signature verifiable by a public key cannot have been produced in any other way than by the user's action on that device.

Verifiable Credentials



Ref: Verifiable Credentials Data Model 1.0



Ref: ISO/IEC/ITU-T X.509

One of the hottest topics in digital identity today is *Verifiable Credentials*.

A Verifiable Credential is simply a signed assertion that certain facts (usually referred to as *claims*) go with a certain actor, the *subject* of the credential.

When the credential includes a public key, then any artifacts signed by the matching private key—and any actions that go with those artifacts—are consequentially bound to those facts.

Verifiable Credential technology is very cool, and it's being standardised at the W3C, but it's not a new pattern. Today's orthodox Verifiable Credential (W3C schematic at left) is functionally the same as the x.509 certificate from the 1990s (right).

Not a new idea

The world's first verifiable credentials were arguably SIM cards and Chip-and-PIN cards. It is useful to recap the contribution these devices make to securing whole classes of business transaction, because this reminds us how to deploy verifiable credentials within existing business contexts.

SIM Cards

The IMSI (the global mobile subscriber ID) is digitally signed by the mobile network operator and secreted inside the SIM chip. When you make a call, your SIM signs a record at the start of the call, which binds your subscriber details to the call, and allows accurate billing worldwide.

Chip-and-PIN Cards

Chip cards are superior to magnetic stripe cards because the chip is active in each payment transaction. A chip card carries exactly the same PAN (the credit card primary account number) as a mag stripe card but grants the number provenance. The PAN is first signed by the issuing bank and secreted inside the chip. Each time you pay at a terminal, the chip digitally signs the purchase data with your private key bound to the PAN.

The static signature of the bank provides provenance; the dynamic signature of the card (which we can assune has been unlocked by the proper customer) proves possession.

The signed purchase data sent into the card system backend for processing is a bundle that cannot have been generated by any means other than the correct customer using a genuine smartcard.

Next: Authenticity of Things

Ref: *The Identity of Things: We're Gonna Need a Smaller Idea*, Steve Wilson, AuthenticateCon 2021.

As I mentioned at FIDO Authenticate 2021, we risk more confusion with the "identity of things". Let's be careful and specific about what we're trying to achieve.

Is it really the "identity" of things? We made a mess of the identity of *people* online and they really have identities.

Remember that a Verifiable Credential binds an important fact about an actor to the actor and to the origin of the fact, so the holder can in turn bind that fact to things they do. A real-world credential (such a bank account, a professional membership, or an official position in a corporation) generally confers some sort of power or authority. A cryptographically Verifiable Credential allows you to exercise that power digitally, by signing artifacts and thus marking those artifacts to precisely reflect your authority to act.

When the actors are smart devices, carrying credentials issued to non-human subjects, the possibilities really open up.

Next: Authenticity of Things

Smart devices need to prove their properties to one another if they are to interact fully autonomously. Verifiable Credentials for devices (as non-human actors) will enable them to act with appropriate accountability based on such properties as ownership, manufacture, specifications, compliance certificates, mechanical performance, service history, jurisdiction, payment of licence fees and so on.

Verifiable Credentials using keys embedded in devices will be critical to addressing fidelity and truth. Digital photographs can be signed in the sensor to make them tamper resistant and convey their origins. A human photographer's credential could be invoked to impart copyright.

Items moving through supply chains (including data records themselves) can bear the mark of each processor at each stage.

In the IoT, instead of "identity of things" we should design for *information about things*.

Authenticity more broadly

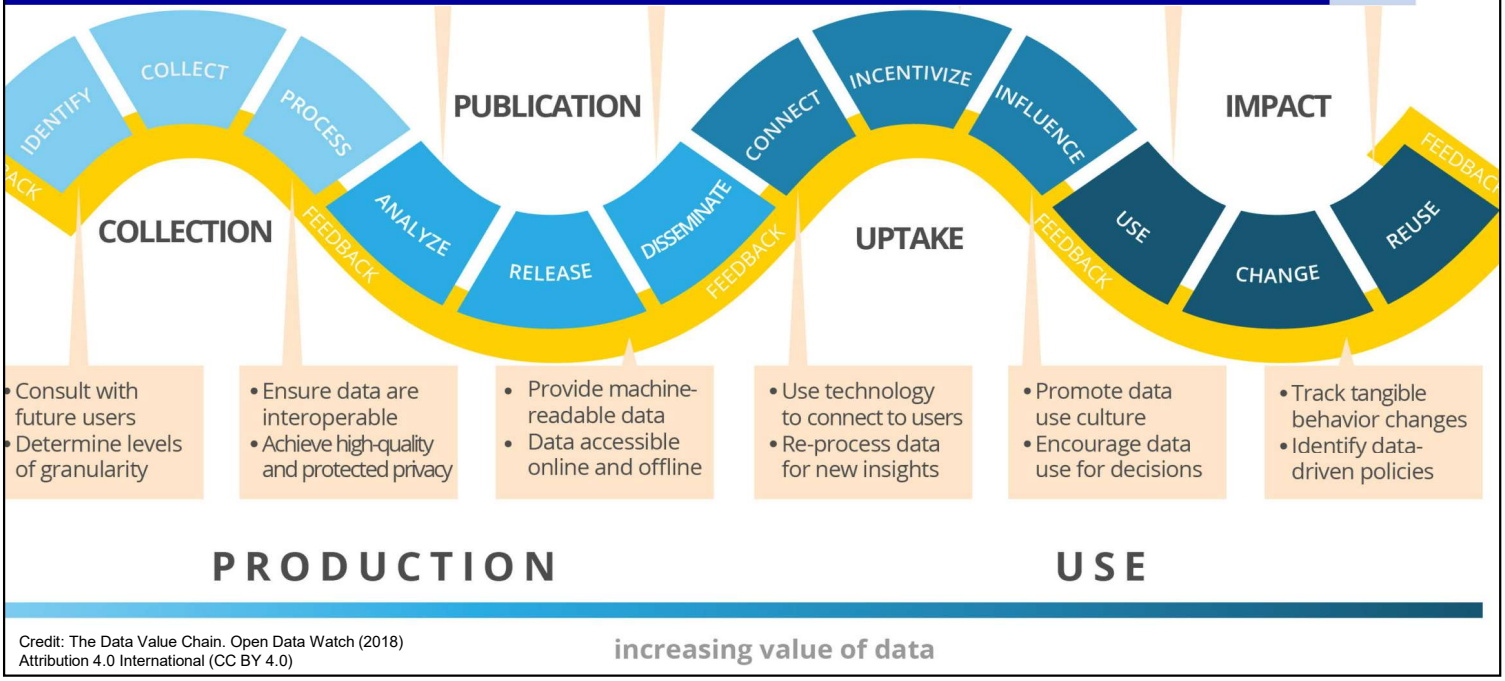
Authenticity is a bigger idea than authentication and could be the next frontier for the FIDO alliance.

The world is gripped by concerns for fidelity, provenance and authorisation throughout the digital economy. Complicated information value chains now extend from raw data sources through multiple value-added processing stages to end users at many different end points, including browsers, mobile devices and special purpose client software. Counterfeits, disinformation, fake news, social media bots and other digital distortions are all enabled by tampering with data.

Authenticity is in the eye of the beholder, as different properties matter in different settings. But whatever properties of a data stream are determined in a use case to be important, those properties can be imparted on data records by well-managed digital signatures, and can be verified at any end-point with access to the right public keys and metadata. These capabilities are core to the protocols FIDO has developed to date with a focus on authentication.

Authentication is traditionally concerned with proving claims about individuals but the FIDO standards and patterns can be extended to proving a much broader range of properties about devices or about data itself. Authenticity boils down data and metadata: proofs that make core data traceable, accountable, reliable and valuable.

Information supply chains



Credit: The Data Value Chain. Open Data Watch (2018)
Attribution 4.0 International (CC BY 4.0)

Monetising data has obviously become an industry – right or wrong, for good and for bad. Data is big business indeed.

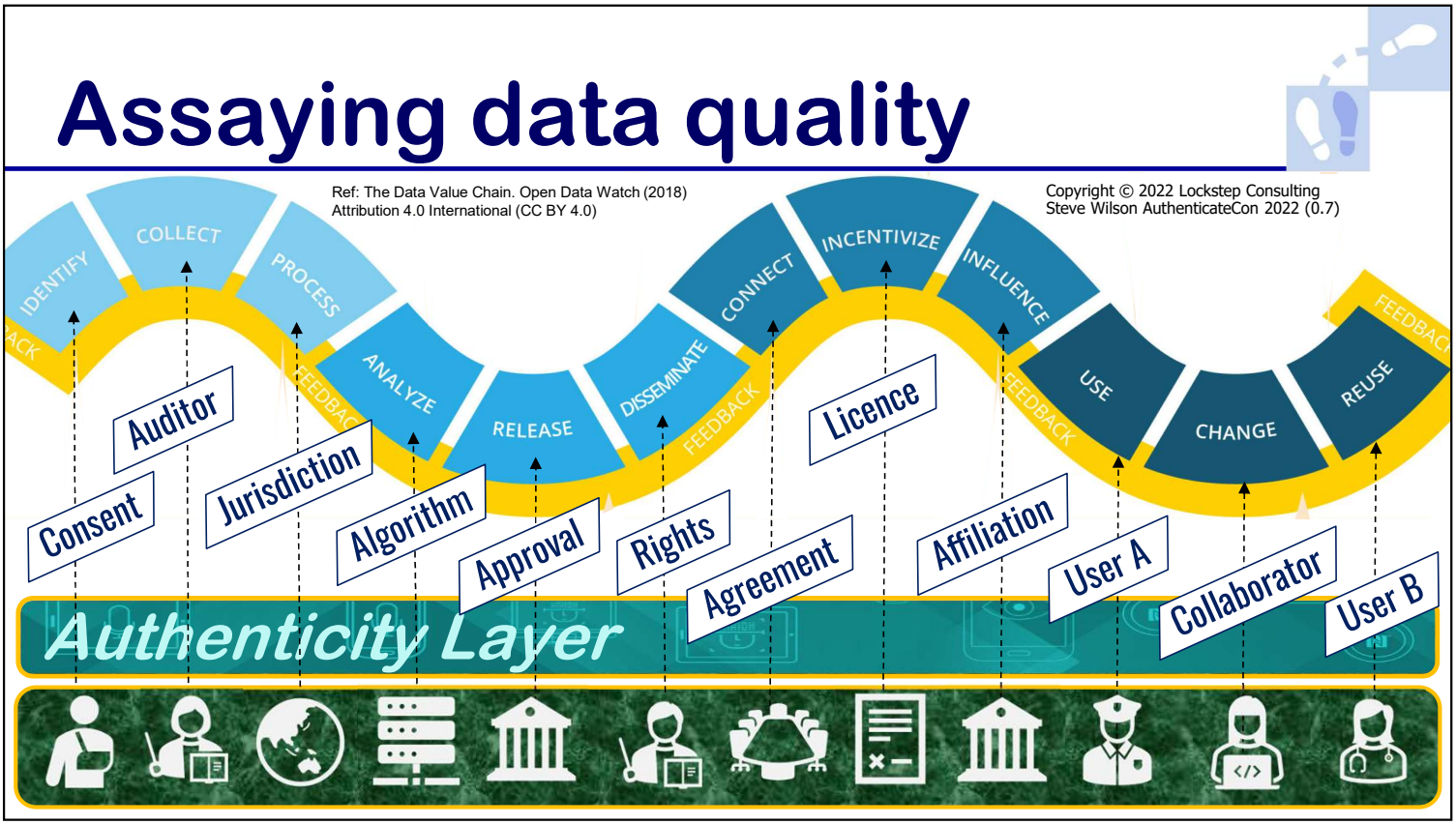
Data supply chains – aka *information value chains* – have been forming under our noses now for decades. They start with various forms of data collection, and proceed through successive stages of filtering, processing, amalgamation, analysis, publication, dissemination and take-up.

Multiple parties touch the data along the way and must be authorised to do so. But what interests us here is not gatekeeping so much as tracing how value is added to data records according to the contributors' roles and authority. So, authorisation is not just a matter of defensive security; it is also key to protecting the value of data, maximing the value, and conveying value to those that consumer data.

We have the tools from Identity Management and from the FIDO Alliance to generate the *metadata* needed to prove who did what to data, when and where, throughout the supply chain.. Edge computing plus cloud APIs will enable all important actors in a data supply chain (be they human or machine) to leave their mark on all important data transformations.

Data is often likened to a raw resource or a utility. We can now conceptualise in detail how to protect data as a resource through its supply chain journey.

Assaying data quality



To focus our thinking about data as a utility, we should ask **what is it that matters about a given data record?** What are the precise qualities make data valuable? And how do we protect those qualities? This framing leads to a larger vision for *data protection*. The qualities of interest vary from one context to another, and might include for example:

- In the case of identifiable (personal) data, the individual's consent to process.
- Details of the data collection process, ethics approval, or instrumentation as applicable.
- Algorithms (incl software version numbers) used for analytics or automated decisions.
- When data processing has been audited, then attach the auditor's signoff.
- Sometimes location or jurisdiction are important.
- As data is added to, who were the contributors, and what were their affiliations?
- The release of data to the public or to specific user communities may specific approval.
- When data, is released, what are the rights that attach to it for further use or distribution?
- Have receivers signed relevant usage agreements or licences?

So, it's not just what you know, but *how do you know*? How do you know what data is intended to be used for, and what conditions attach?

These questions typify how we can frame data as a utility, and to start to think about we might *assay* it, so that the important properties are protected, legible and accountable.

Conclusion: Leading at the edge

In summary, the FIDO Alliance membership is highly representative of both the buy and sell sides of the digital economy, as well as technology vendors and services, from major cloud providers, mobile platforms and operating systems through to chip manufacturers.

FIDO has helped to normalize a cryptographic technology stack in mobile phones and devices, enabling Verifiable Credentials and personal data wallets, and in the medium term, the embedded key chains that will allow autonomous IoT devices to work each other out.

There is so much more to authentication than identity. The internet is not missing an "identity" layer so much as an *authenticity layer*, to convey the originality of any information, protect its fidelity and maximise its reliability. And so we are coming to a more comprehensive new understanding of data protection, across everyday digital experiences, online business, the Internet of Things, and all of cyberspace. The cryptographic signals needed to convey and verify authenticity will be generated at the edge, and verified at the edge, as all end points in the digital economy come to be aligned to standards like FIDO.