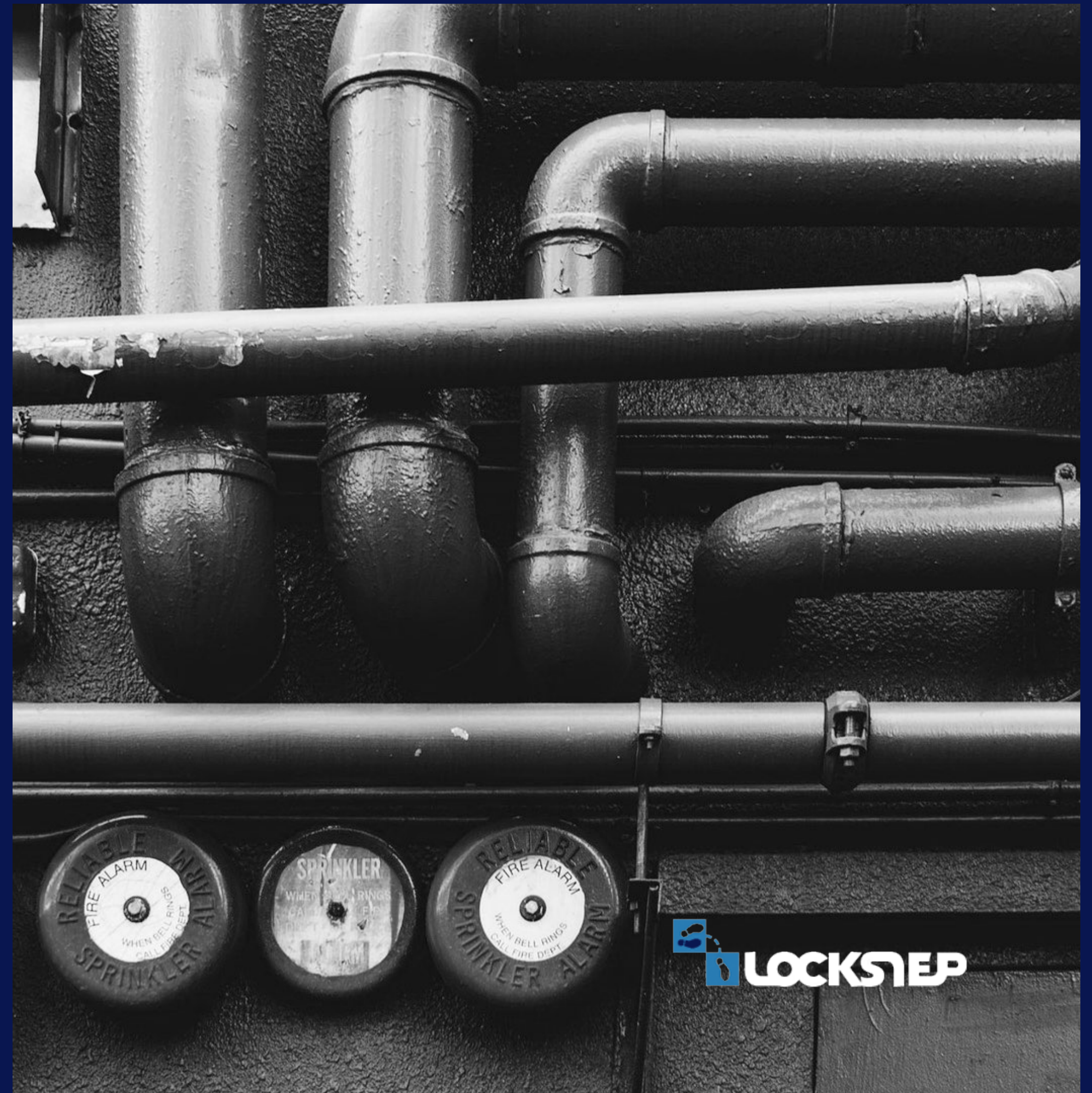


Stephen Wilson, Lockstep Consulting
with George Peabody, Glenbrook Partners

Trust in the post-identity world

November 2022



The digital discourse is dominated by identity

Until recently, identity was all we had to go on when trying to trust anyone or anything online. We developed a terrible habit of over-identifying.

Relying parties collect circumstantial clues like credit card verification codes and social security numbers instead of properly verifying what really matters.

People divulge too much personal data, often unwittingly, which leaks and gets abused by criminals.

Too much identity is sloshing around.

The most important developments in our industry — self-sovereign identity, the FIDO Alliance, and cryptographically verifiable identities — aren't really about identity, but authorship, provenance, integrity and control.



Is a paradigm shift coming?

What if we move the conversation beyond identity?

Imagine a world where cryptographic infostructure is as universal as electricity or clean water, and all the data we need is hallmarked, traceable, and trustworthy thanks to authentication technologies.



We must end our obsession with “identity”

I say this with love and respect for my dear friends in the industry, but...

For thirty years, identity has dominated digital practice and discourse.

We overcook the Peter Steiner cartoon. It was just a fantastical gag about dogs getting up to mischief, not a commentary on digital trust.

For all that time, when trying trust anyone online, we only had identity to go on. When faced with higher risk, we would seek higher trust and ask for more identity. We put quantity of identity ahead of quality. We put identity first.

The received wisdom in our industry holds that a “missing identity layer” is the Internet’s “original sin”

Image: Peter Steiner/CartoonStock.com



“On the Internet, nobody knows you’re a dog.”

We developed terrible habits

A close-up photograph of a metal ashtray overflowing with discarded cigarette butts. The butts are of various colors, including orange, white, and yellow, and are scattered across the surface of the ashtray. Some butts are still lit, while others are completely smoked. The background is dark and out of focus.

Instead of verifying the facts that really matter about the people we deal with, we drag in extra identifying data from unrelated contexts such as CVVs and SSNs — much of which is then stolen and bought and sold and replayed by fraudsters.

Consider knowledge-based authentication, which places a premium on “out of wallet” details which should be less likely to be known to criminals. But personal information is everywhere on the Internet and KBA backfires by motivating a black market for personal data.

Identification for digital risk management can be like putting out fire with gasoline. We should do more to secure the facts and figures that transactions depend on.

Regulatory pressure is building

Demand is growing for transparency and accountability of data flows, processing, and consumer understanding. No more Wild West!

Data rights
Open banking
Data localisation
Algorithm accountability



Help prevent truth decay

Phishing
Card Fraud
Deep Fakes
Romance Scams
Synthetic Identities
Weaponisation of Information

Cynics say we are post truth but surely the biggest challenge as cyberspace grows in importance really is digital truth.

From payment card fraud and online scams through to misinformation and AI-driven Deep Fakes: every one of these problems is fundamentally about poor quality data.

We can't trust the evidence of our own eyes anymore. Are we really going to launch digital twins without taking better care of fidelity?

Taking the first steps



C2
PA

Coalition for
Content Provenance
and Authenticity


Verified Information Exchange

ge

Concerted multidimensional responses to the data quality problem are underway, as are some narrow legislated bans on deep fakes.

Several major mastheads have teamed with Microsoft Research in a content provenance coalition. The **C2PA**'s first draft standard draws heavily on technical measures familiar to the identifierati, such as digital signatures.

And the new **Verified Information Exchange** (VIE) is an interdisciplinary research program hosted by UW. The VIE work program suggests that network (i.e. scheme-based) business models are emerging for data supply.

A photograph of a busy outdoor market stall. In the foreground, a woman with long dark hair, wearing a white floral-patterned blouse and a watch, is reaching out to inspect produce. An older man with glasses and a striped shirt is also looking at the goods. The stall is filled with various fresh fruits and vegetables, including tomatoes, grapes, and leafy greens. In the background, other market-goers and the warm, ambient lighting of the market are visible.

“The global information environment is a form of ‘market’ that needs exchange protocols and local standards.” — VIE

GAIN: verifiable data beyond just identity

GAIN was launched via the Open Identity Exchange. It means different things to different stakeholders. Even the 'I' in GAIN was reframed at Identiverse as interoperability.

The GAIN model has applicability beyond identity to information more generally.

One of its best features is buried on page 42 of 59. The service provider is a fourth party in the data flow, joining the familiar end user, issuer and relying party. It is explicitly likened to the acquirer in the global card payment network.



GAIN DIGITAL T

How Financial Institutions are taking a leadership Economy by establishing a Global Assured Identity

With over 150 co-authors

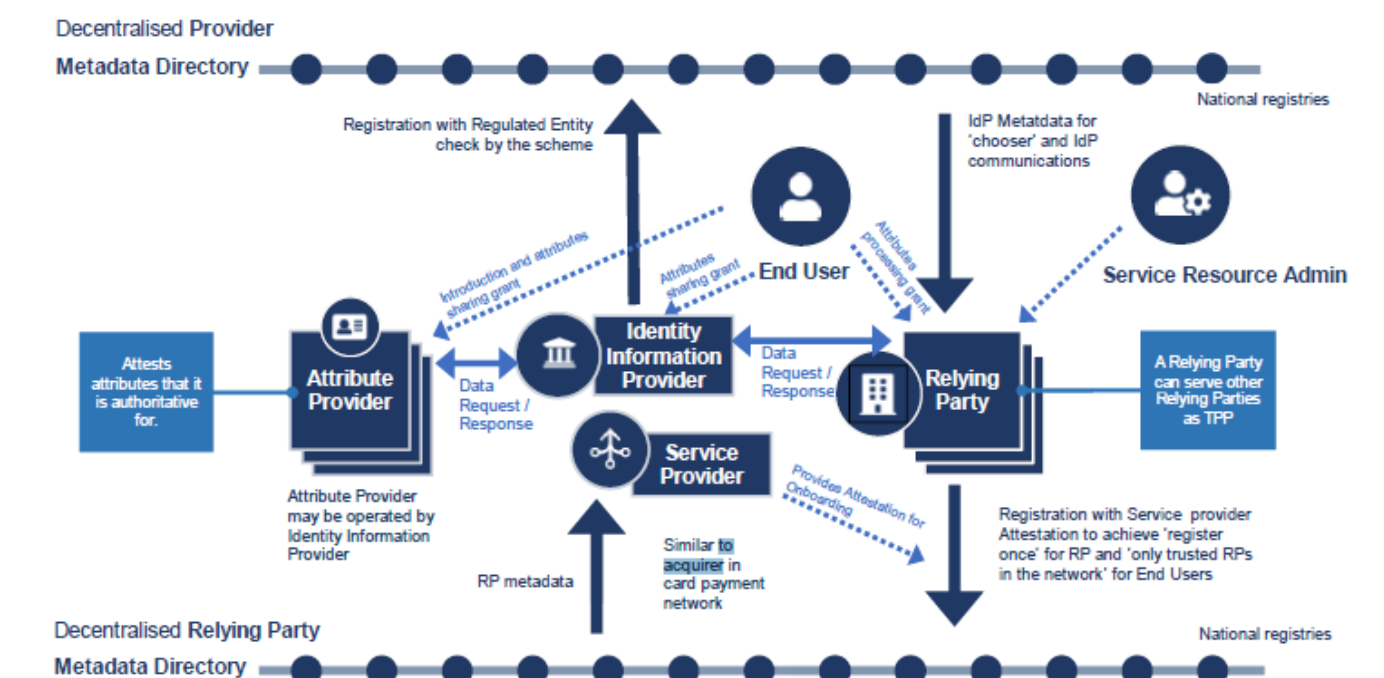
D.3.2.3 Privacy Dashboard

Participating Identity Information Provider in GAIN will provide a dashboard from which the End-Users can find out easily where and which data has and is being shared for what purpose and how. End-Users can review where data has been shared and stop any persistent sharing from within the Identity Information Provider Dashboard.

D.3.3 Data Flow View

Data Flow View provides how the Information including user and administrator direction flows and stored among the roles to be implemented in GAIN.

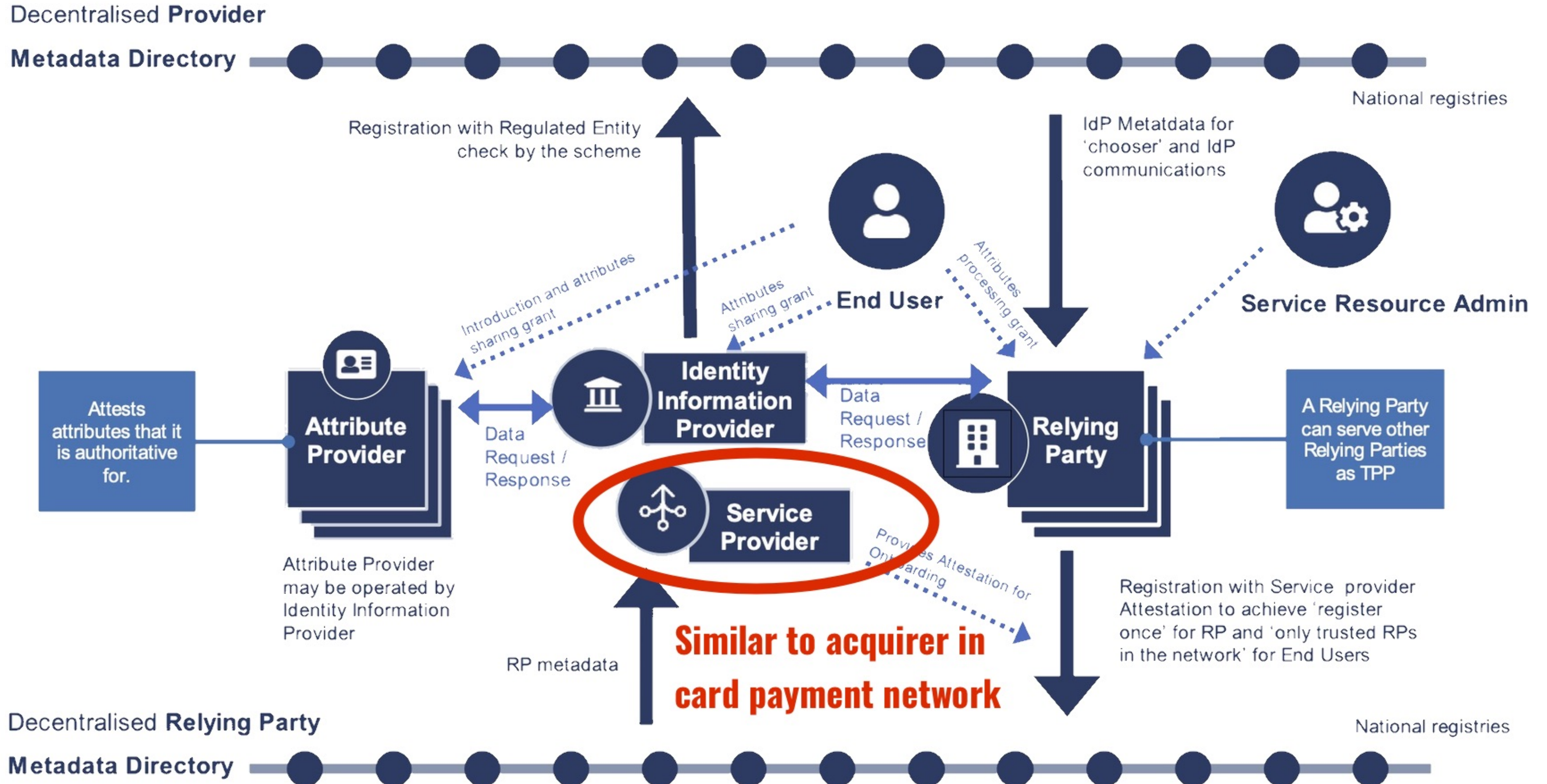
Figure D.4: Data Flow in the GAIN



Note: RP Onboarding requirements may differ from jurisdiction to jurisdiction and it probably requires multiple levels of identity proofing and verification.

- **End-User:** End-User is a role primarily performed by individuals and is the central role in the GAIN. They are authenticated by User-AuthN and control how and where their data is being shared and used.
- **Service Provider:** It is a role that performs initial authentication (identity proofing) of the Relying Party and provides standardized attestation which Relying Parties can take and provide to the Relying Party Metadata Directory. This role is typically played by a regulated entity that has a requirement for identity proofing of the Relying Parties as their customer. It
 - implements the management system to achieve the assurance level expressed in the attestation;
 - support mapping of the Relying Party to a Legal Entity Identifier (LEI)³⁰ and a verifiable LEI (vLEI)³¹ in partnership with the Global Legal Entity Identifier Foundation (GLEIF)³²; and
 - support issuing the attestation in the standard format adopted by GAIN that include the information above.

Figure D.4: Data Flow in the GAIN



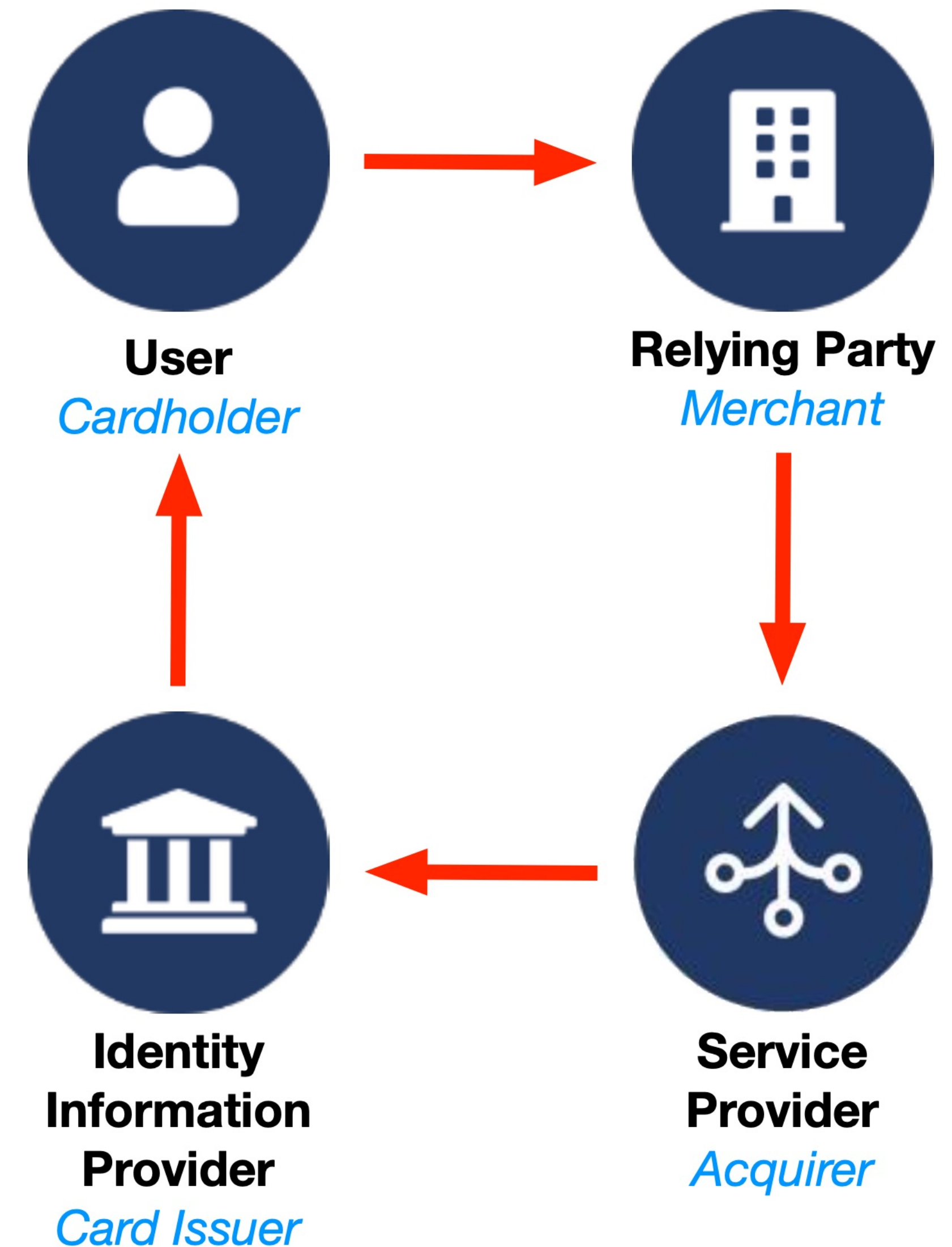
GAIN is infostructure

Payment cards and the processing network exist purely so that certain customer data — account numbers and some metadata — can be reliably presented to merchants and verified.

GAIN represents an extension of the four-party model for presenting and verifying data more generally.

The acquirer is the key to global scalability. The acquirer provides technology and legal support: merchant onboarding, methods to ingest customer details (card terminals, internet gateways and/or APIs) and, above all, a standard form of merchant service agreement with service levels, liabilities and fee structures which can be fine-tuned regionally.

Card schemes are a paragon of infostructure.



The **flow** of identity information and *cardholder details* between **GAIN elements** and *credit card scheme elements*

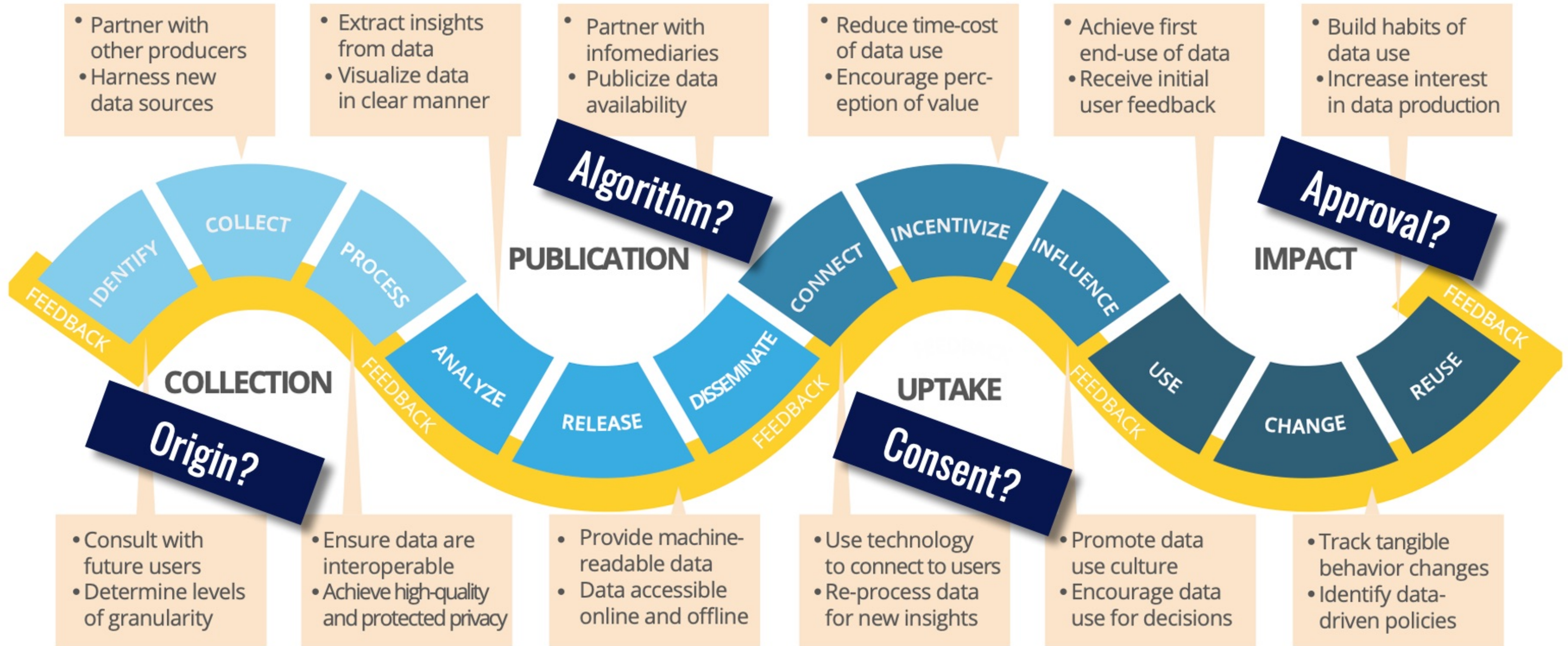
What is infostructure?

“An organizational structure used for the collection and distribution of information; (now usually) the information technology infrastructure comprising hardware, networks, applications, etc., used by a society, business, or other group.”
— Oxford English Dictionary

That is, verifiable data sharing will be underpinned by rules, technologies, and business models.



How do we know we can trust complex data supply chains?



Let's think in terms of assaying data

If there's any truth in the comparison of data and crude oil, then let's start to measure the properties of data that make it reliable, fit-for-purpose, and valuable — at every step.

Then let's bind the assays to the data records as they move through the information value chains.



We have the tools

I envision a world with widespread cryptographic infrastructure.

Verifiable data is available everywhere — just like stable electricity and clean drinking water.

We ID pros know we have these tools, because we've already built them!



The post-identity world

Let's shift focus from the abstract to the concrete. The idea of identity is simply not helping.

That might be counter-intuitive, or strike some as sterile, but pragmatically it doesn't matter.

The digital identity industry has shown us how to design for verifiable facts and protect them cryptographically.



We can trust without identifying

We can break old habits. Instead of starting with identity, let's ask:

What do you really need to know?

Where will you get the data?

How will you know if it's true?

It's perfect timing for a paradigm shift. We have intelligent devices at the edge, we have mobile digital wallets that make ideal verifiable containers for data, and we have clouds full of APIs.



**If zero trust is a thing
then so is zero identity**

Stephen Wilson, Lockstep Consulting
lockstep.com.au
@Steve_Lockstep

