Interoperability Working Group for

Guide to Key Concepts and Terminology

Curated by the GHP Governance Framework Drafting Group

The goal of the Good Health Pass Collaborative is to help reopen global travel by enabling health passes to be as interoperable as passports or credit cards

This starts with harmonizing the terms and concepts used throughout the Good Health Pass digital trust ecosystem

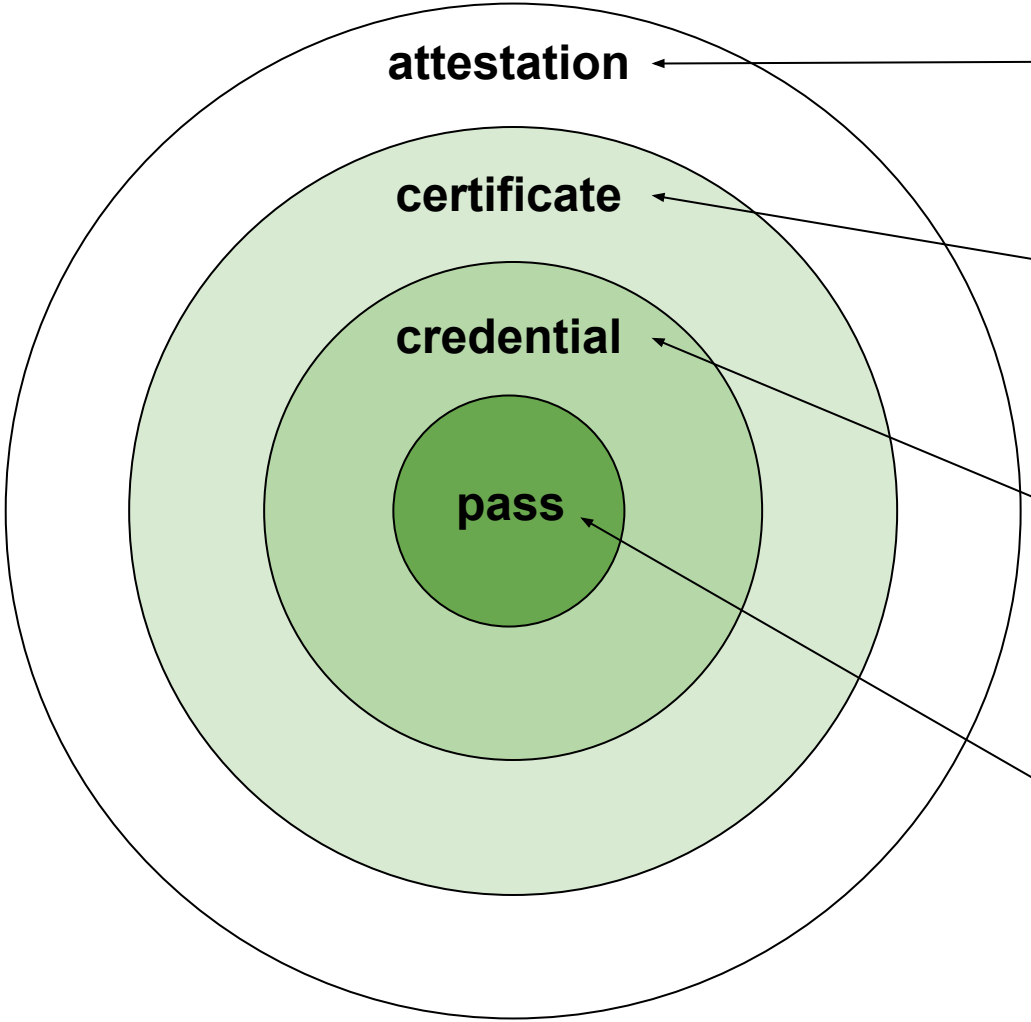
This slide deck will walk you through the Good Health Pass story using the primary terms and concepts we have agreed upon

Part One:
What is a Good Health Pass?

The first challenge is to explain why the initiative is called Good Health Pass

Almost a dozen different terms have been used to describe the container of data a traveller needs to prove their COVID-19 health status

Of these terms, we settled on four to use precisely and consistently in Good Health Pass architecture



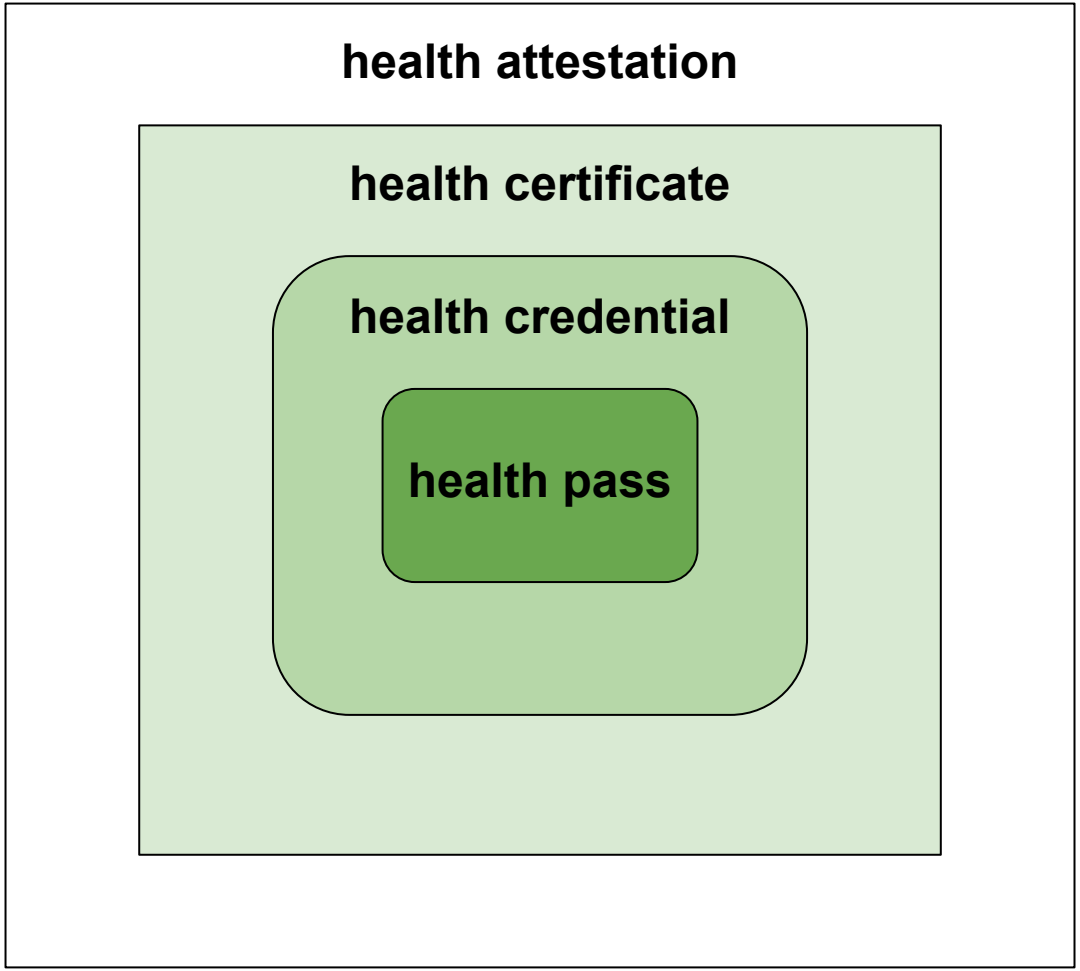
attestation: A set of **claims** about a **subject** for which the attester can be held accountable. This includes a **self-attestation**.

certificate: A set of **claims** about a **subject** by an **issuer** that can be verified in some manner, either manually or automatically. May be either **paper** or **digital**.

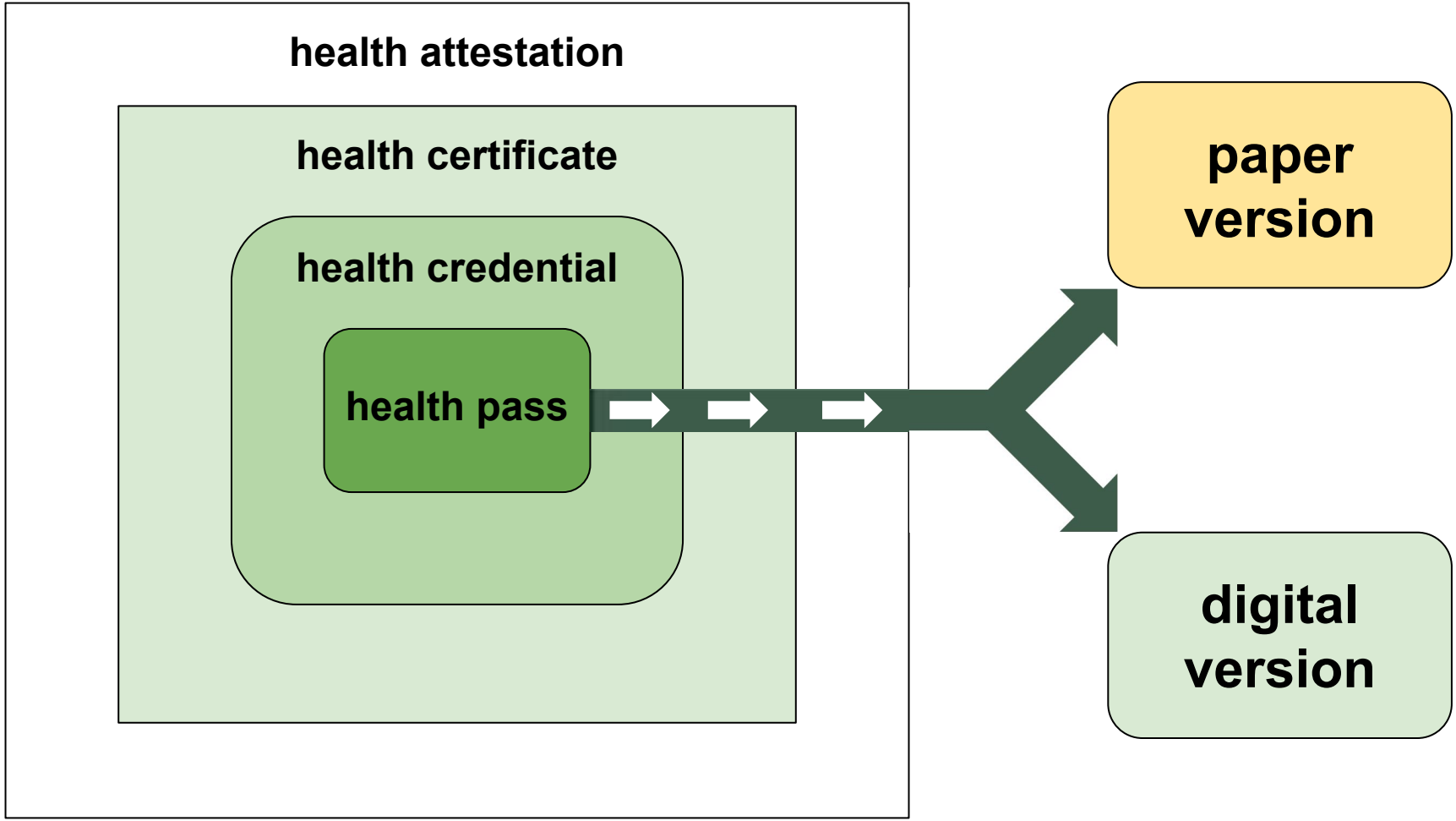
credential: a **certificate** issued in a form designed to be easily transported by the holder and easily verified by a **verifier**, especially using machine-readable data and/or cryptographic signatures.

pass: a **credential** to which **data minimization** and **anti-correlation** have been applied so it includes only the data a **verifier** requires to make a **trust decision** in a specific context (such as boarding a plane).

All four terms can be put in the context of health data


health attestation
health certificate
health credential
health pass

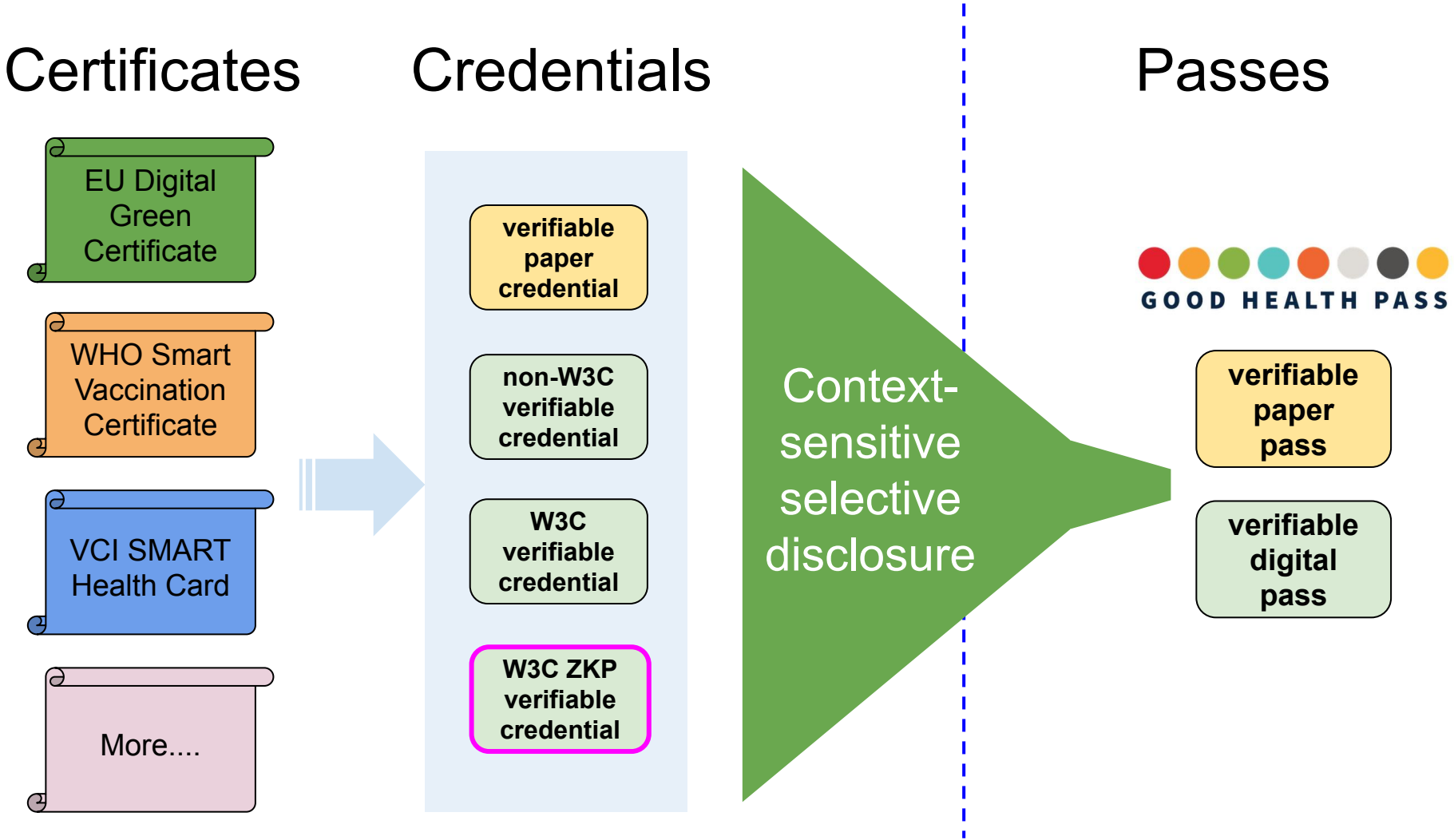
All four of these data containers can also be produced in either paper or digital versions


health attestation
health certificate
health credential
health pass
paper version
digital version

So what makes a health pass a Good Health Pass?

It follows the Good Health Pass Principles—first by being digitally signed so it is verifiable as coming from an authorized issuer

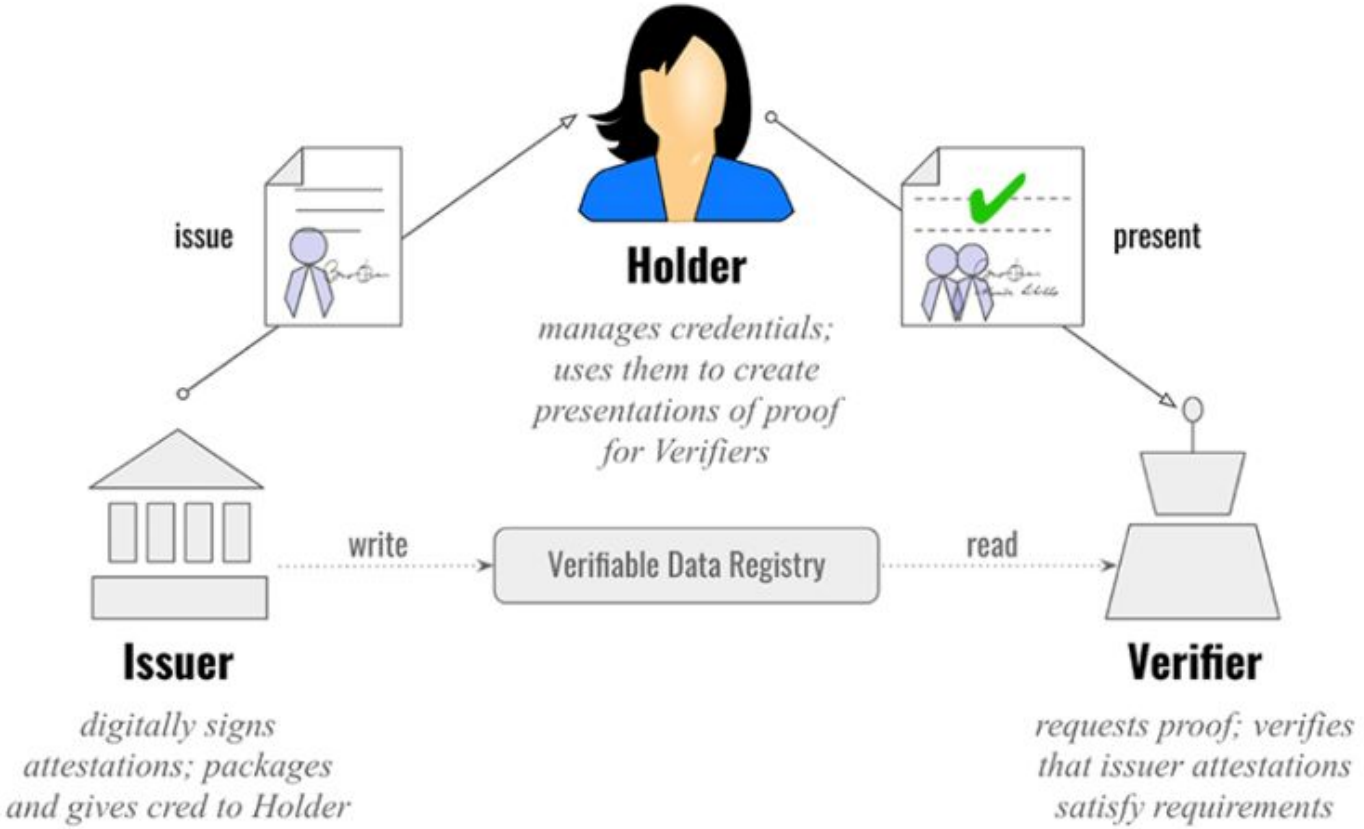
Second by applying data minimization and anti-correlation so it transmits only the data the verifier absolutely needs to know


Certificates
Credentials
Passes
EU Digital Green Certificate
WHO Smart Vaccination Certificate
VCI SMART Health Card
More....
verifiable paper credential
non-W3C verifiable credential
W3C verifiable credential
W3C ZKP verifiable credential
Context-sensitive selective disclosure
GOOD HEALTH PASS
verifiable paper pass
verifiable digital pass

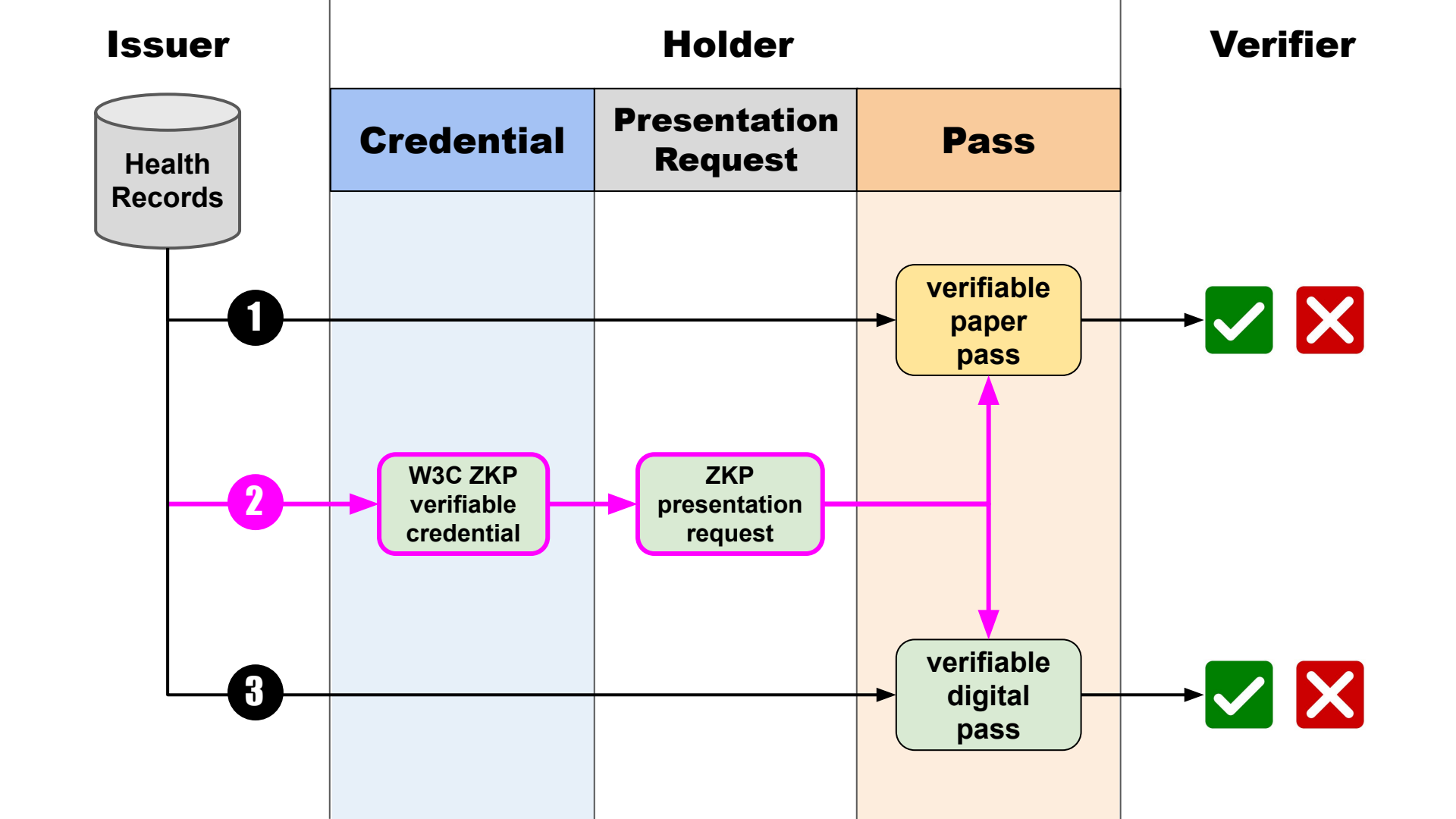
Part Two:
The Paths to a Pass

All health pass solutions follow the classic “trust triangle” model of the W3C Verifiable Credentials specification

The verifiable credential trust triangle

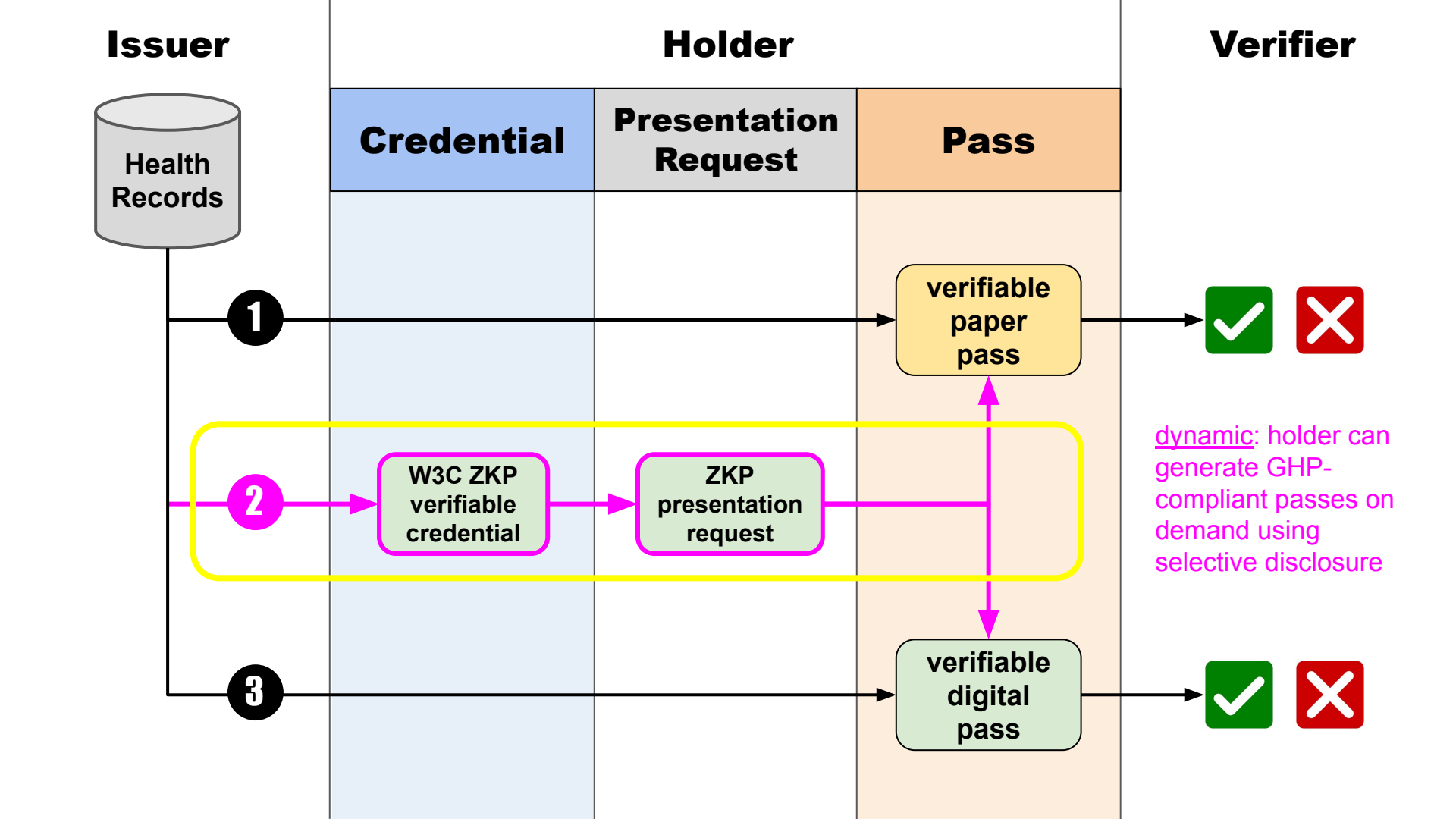


Following this model, there are three paths that can be taken to directly issue a GHP-compliant health pass so it can be verified using the signature of the original issuer


Issuer
Holder
Verifier
Health Records
Credential
Presentation Request
Pass
1
2
3
verifiable paper pass
W3C ZKP verifiable credential
ZKP presentation request
verifiable digital pass

The first and third paths are static—they require the issuer to already know the precise minimal set of data the holder requires in a health pass— a burden many issuers (such as EHRs) may not be in a position to bear

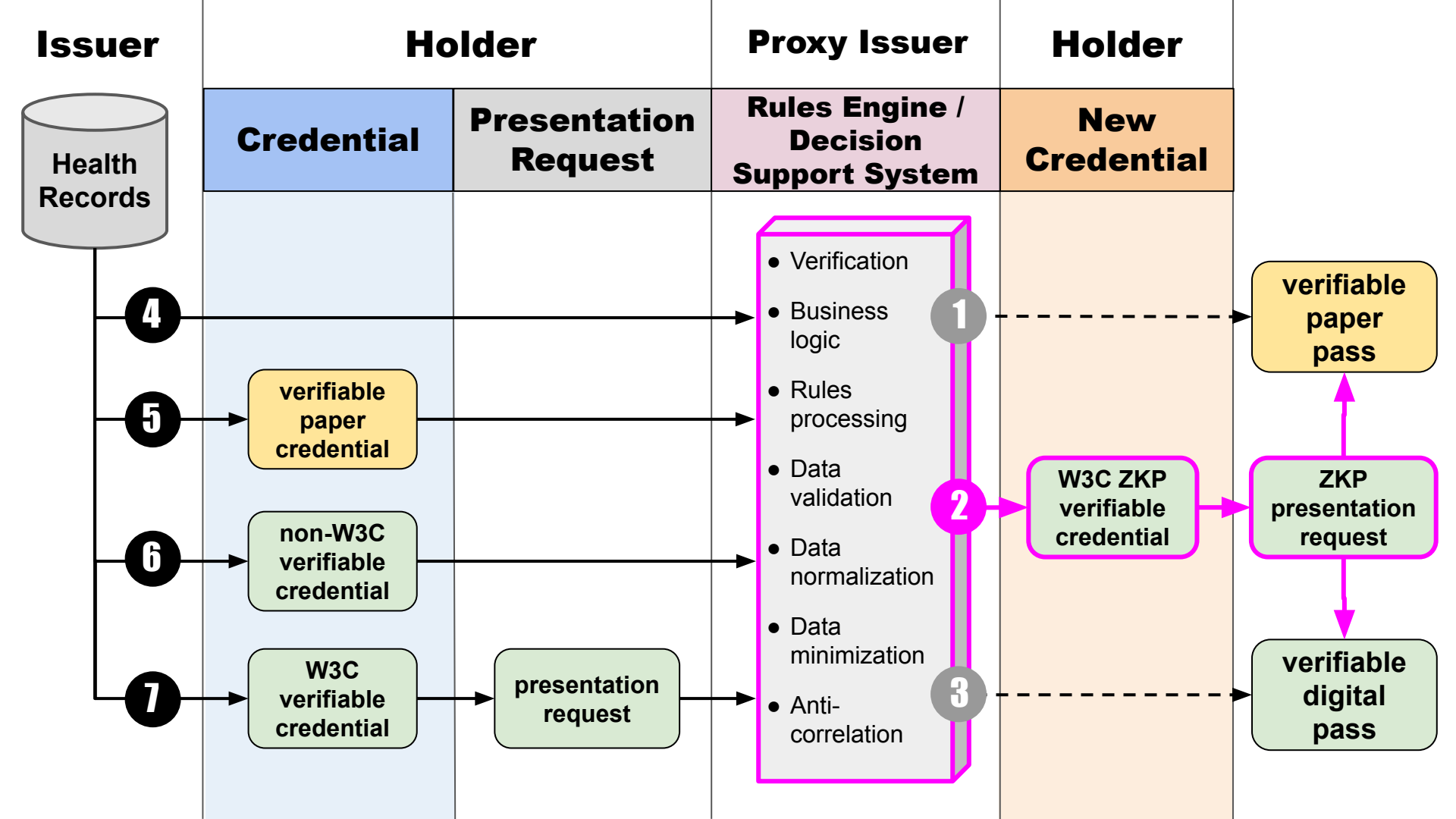
But the second path is dynamic—it uses zero-knowledge cryptography (ZKP) to enable the holder to selectively disclose only the data the verifier needs to know in a specific context (such as boarding a plane)


Issuer
Holder
Verifier
Health Records
Credential
Presentation Request
Pass
1
verifiable paper pass
2
W3C ZKP verifiable credential
ZKP presentation request
dynamic: holder can generate GHP-compliant passes on demand using selective disclosure
3
verifiable digital pass

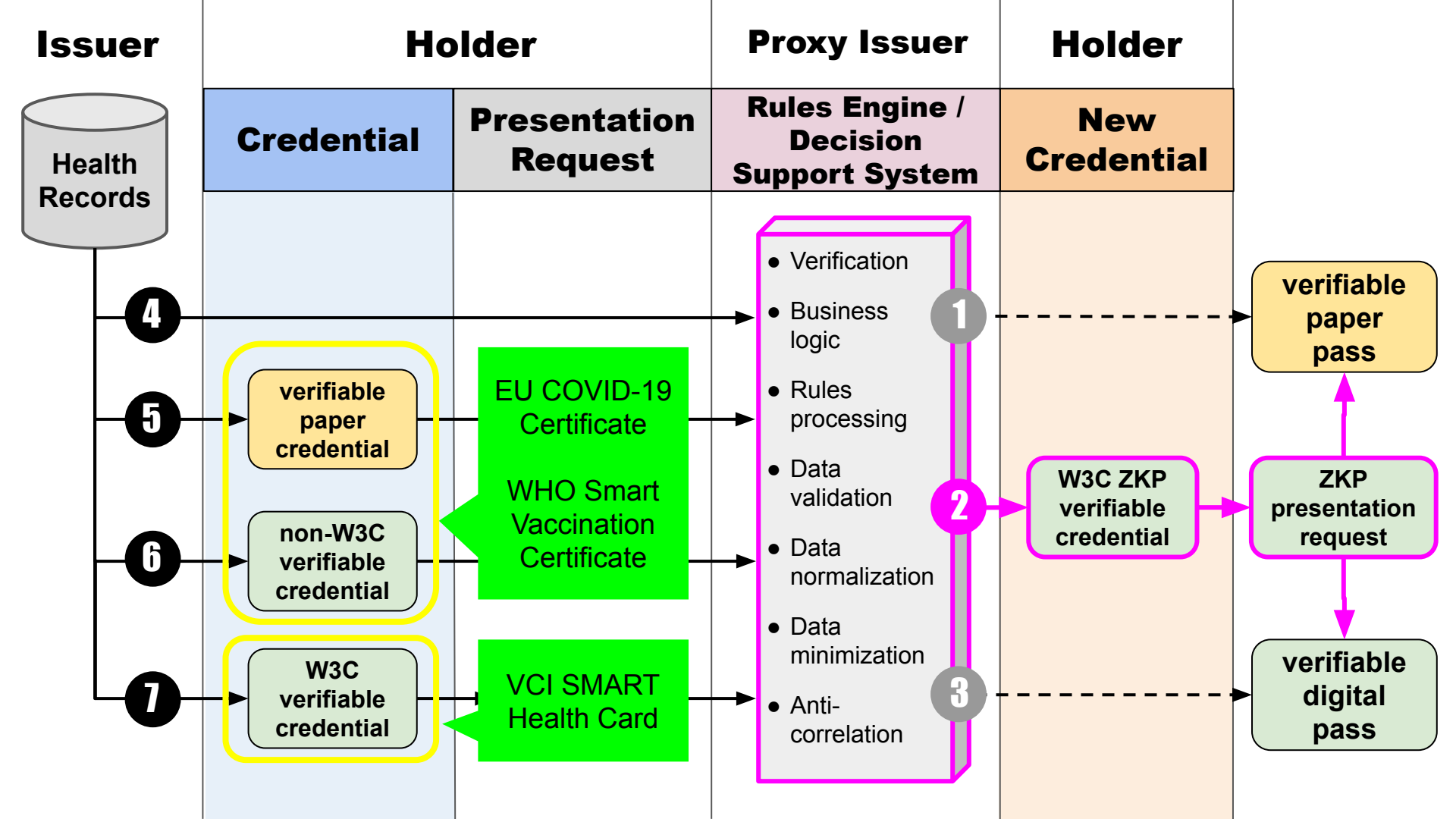
However these first three paths do not support the wide variety of health certificates and credentials that are already being mandated or issued by governments or health authorities

These include the
EU COVID-19 Certificate,
the WHO Smart Vaccination Certificate,
and the VCI SMART Health Card—
as well as a growing number of others

To accommodate these, there are four more paths that use a proxy issuer to verify the original health certificate(s), credential(s)—or even self-attestations—before issuing a new GHP-compliant credential or pass


Issuer
Holder
Proxy Issuer
Holder
Health Records
Credential
Presentation Request
Rules Engine / Decision Support System
New Credential
4
5
6
7
verifiable paper credential
non-W3C verifiable credential
W3C verifiable credential
presentation request
Verification
Business logic
Rules processing
Data validation
Data normalization
Data minimization
Anti-correlation
1
2
3
W3C ZKP verifiable credential
verifiable paper pass
ZKP presentation request
verifiable digital pass

Paths #5, #6, and #7 are explicitly designed to accommodate existing or planned health certificate or credential formats and signature types (including X.509 public key directories)

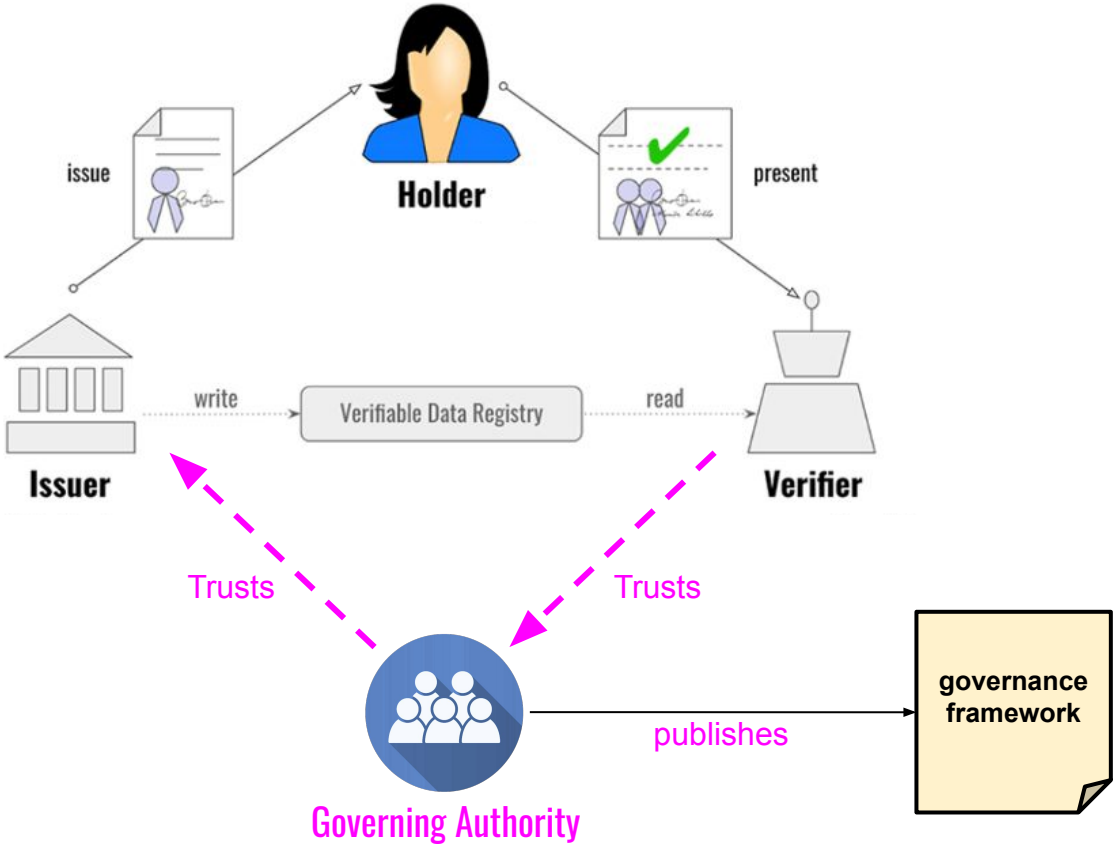

Issuer
Holder
Proxy Issuer
Holder
Health Records
Credential
Presentation Request
Rules Engine / Decision Support System
New Credential
4
5
6
7
verifiable paper credential
non-W3C verifiable credential
W3C verifiable credential
EU COVID-19 Certificate
WHO Smart Vaccination Certificate
VCI SMART Health Card
Verification
Business logic
Rules processing
Data validation
Data normalization
Data minimization
Anti-correlation
1
2
3
verifiable paper pass
W3C ZKP verifiable credential
ZKP presentation request
verifiable digital pass

Part Three:
Governance Frameworks and Trust Registries

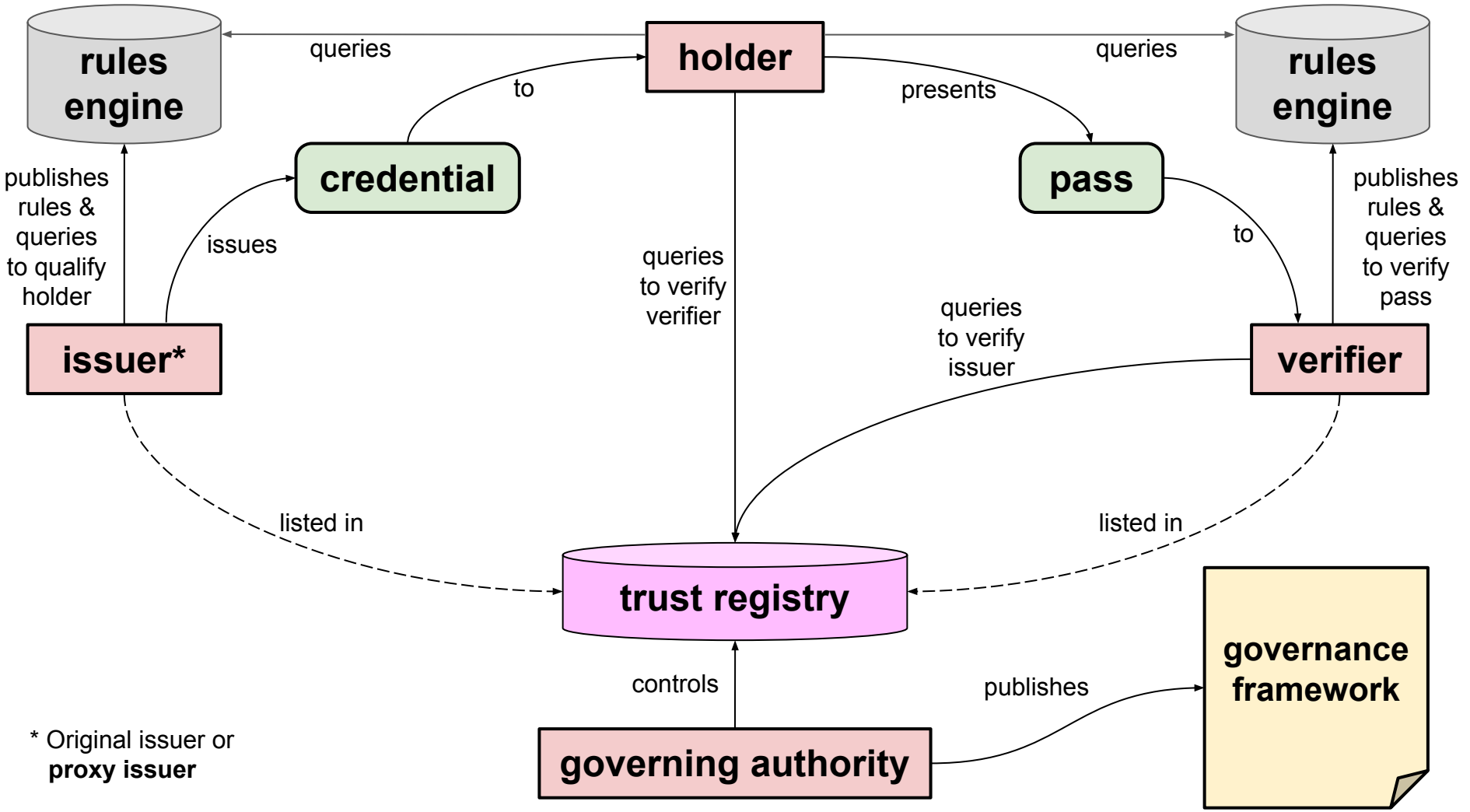
To support a multi-party digital trust ecosystem, the trust triangle of issuers, holders, and verifiers needs governance

This is the role of a governing authority responsible for developing, publishing, and maintaining a governance framework

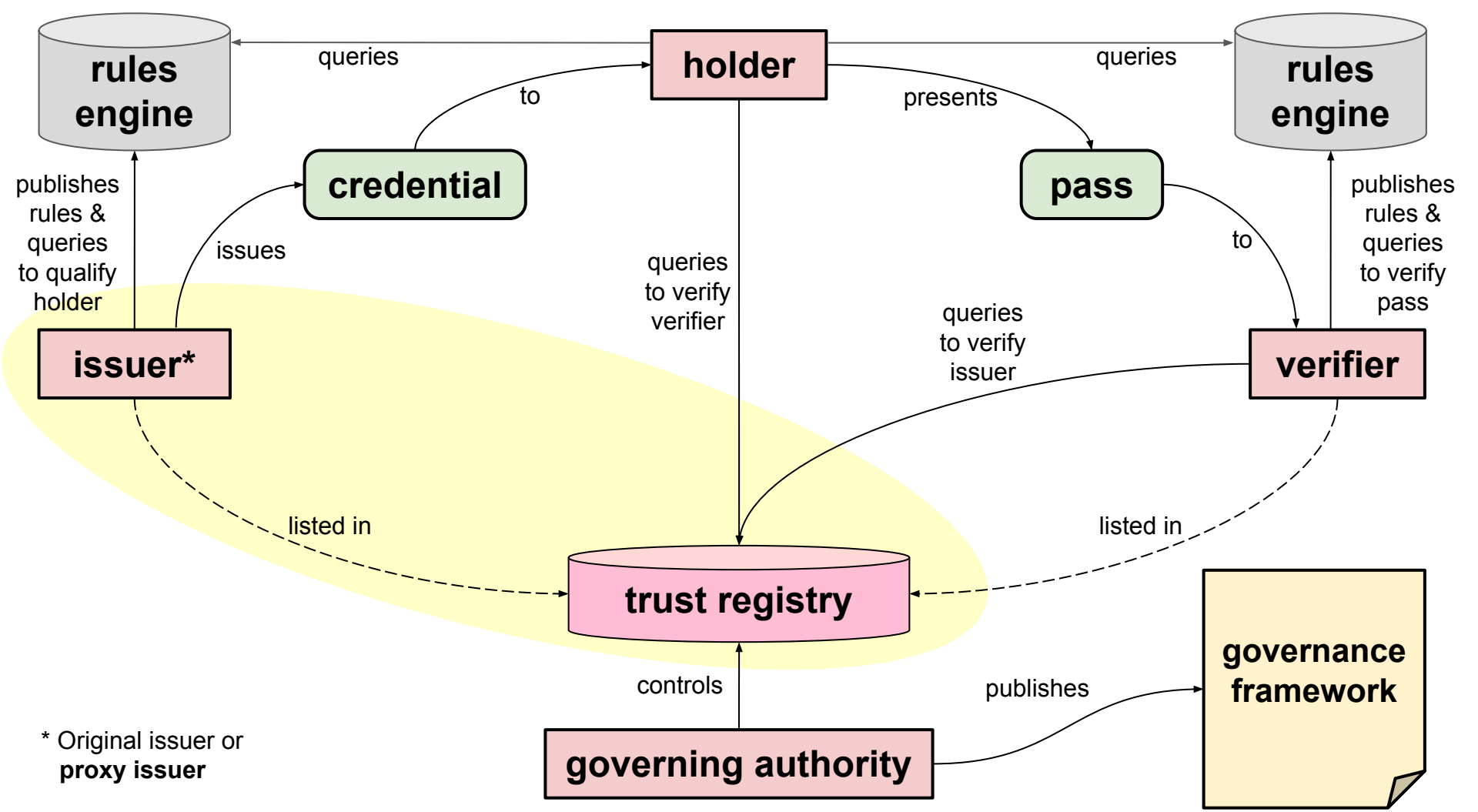
The governance trust diamond



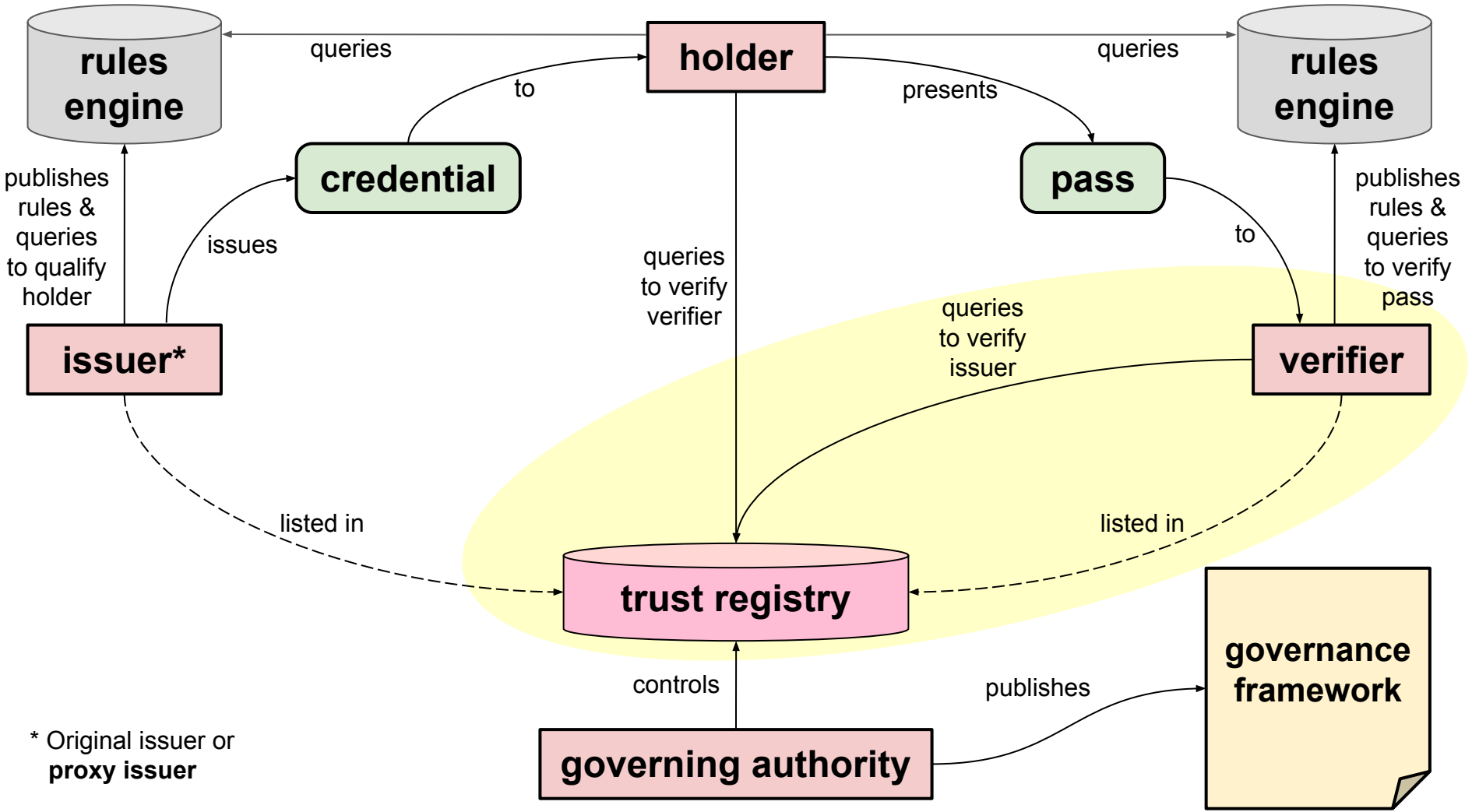
To enable the ecosystem to scale,
members need to be able to quickly verify
who is authorized to do what—
this is the role of a trust registry


rules engine
queries
holder
queries
rules engine
to
presents
credential
pass
publishes rules & queries to qualify holder
issues
queries to verify verifier
to
publishes rules & queries to verify pass
queries to verify issuer
issuer*
verifier
listed in
listed in
trust registry
controls
publishes
governance framework
governing authority
* Original issuer or proxy issuer

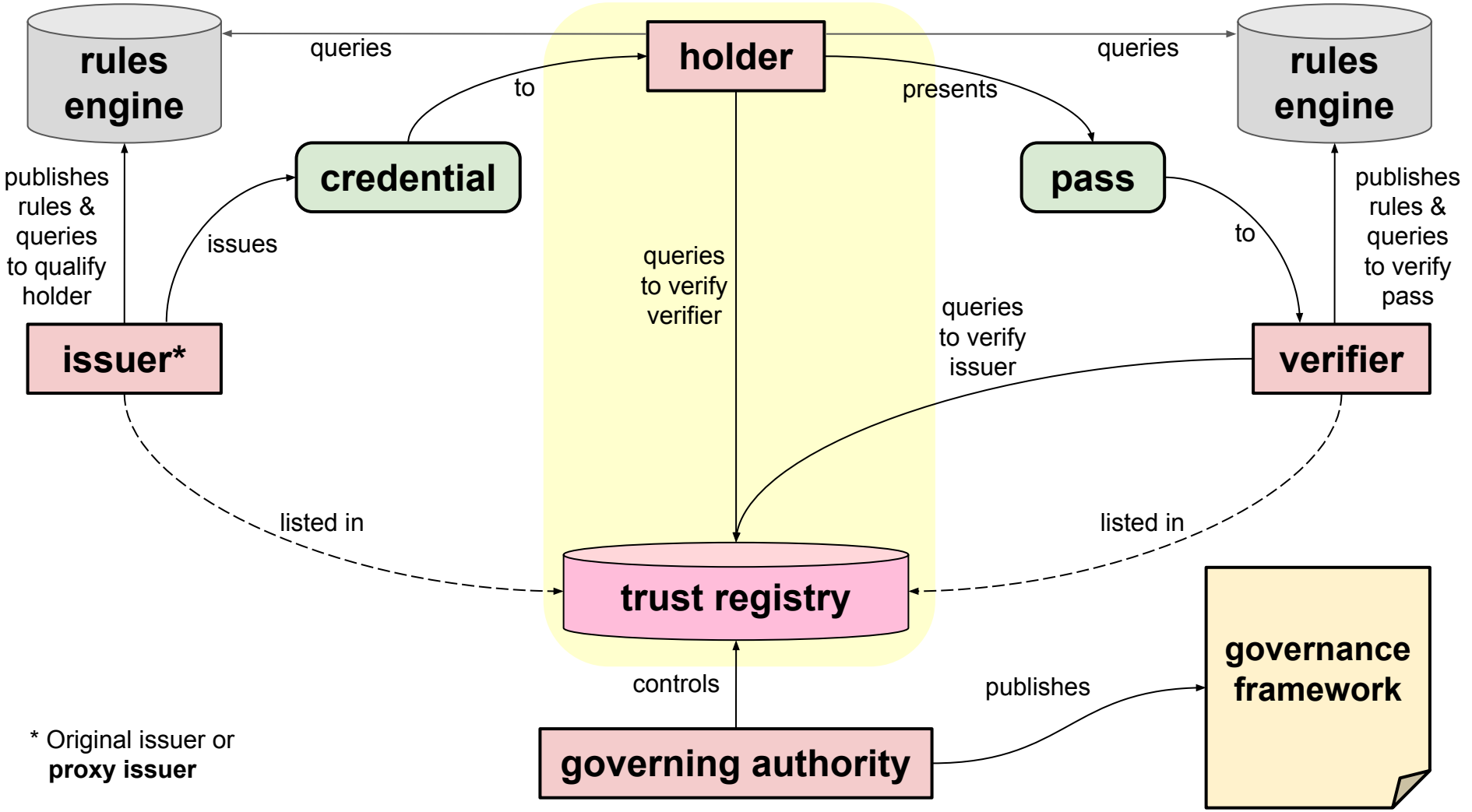
The trust registry maintains a list of all authorized issuers in the ecosystem and the types of credentials and passes they are authorized to issue


rules engine
queries
holder
queries
rules engine
to
presents
credential
pass
publishes rules & queries to qualify holder
issues
queries to verify verifier
to
publishes rules & queries to verify pass
queries to verify issuer
issuer*
verifier
listed in
listed in
trust registry
controls
publishes
governance framework
governing authority
* Original issuer or proxy issuer

When a verifier is presented with a pass, the verifier can use the issuer ID and pass type to query the trust registry and determine if the verifier is authorized


rules engine
queries
holder
queries
rules engine
to
presents
credential
pass
publishes rules & queries to qualify holder
issues
queries to verify verifier
to
publishes rules & queries to verify pass
queries to verify issuer
issuer*
verifier
listed in
listed in
trust registry
controls
publishes
governance framework
governing authority
* Original issuer or proxy issuer

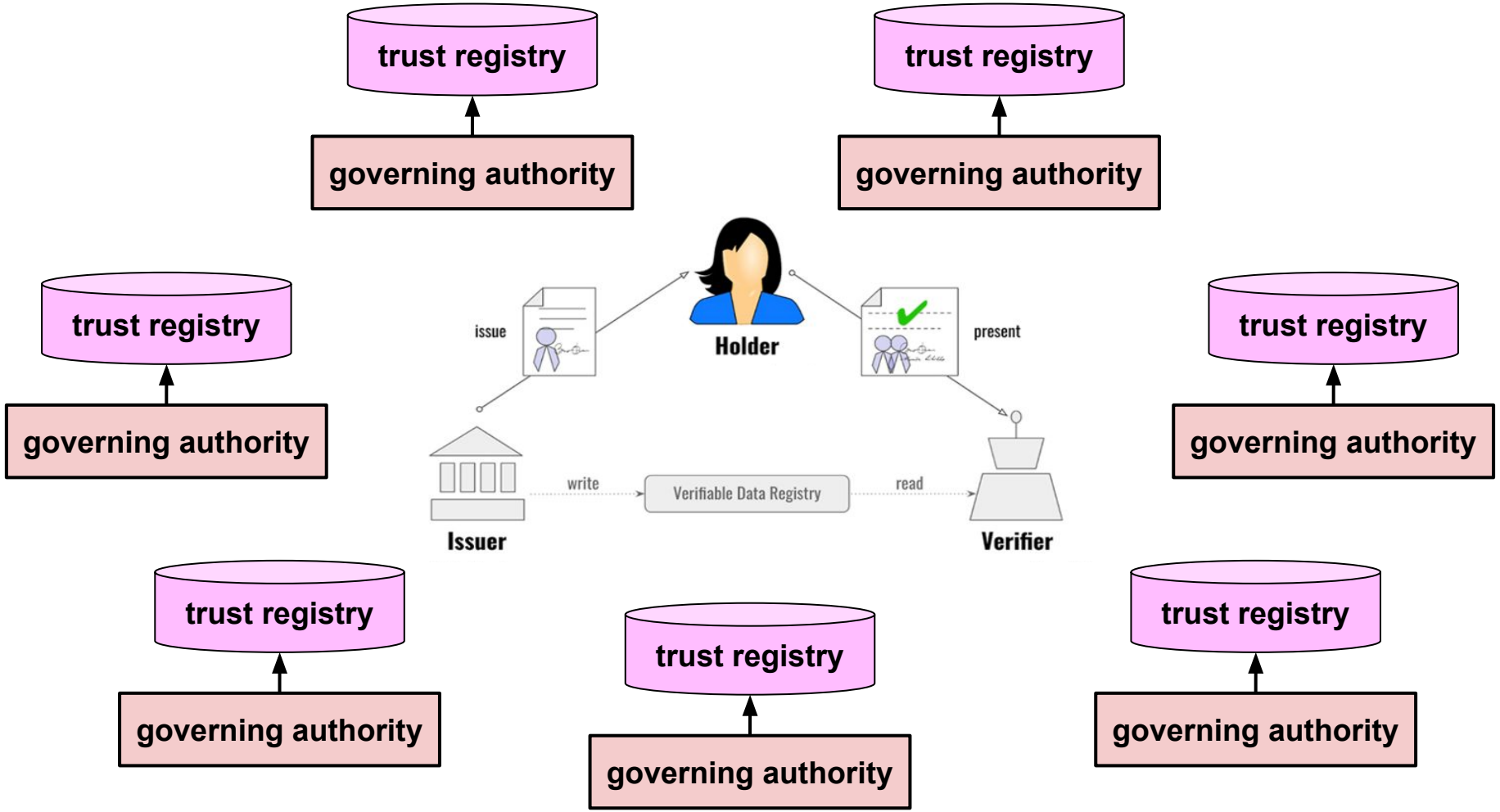
Some governance frameworks also require verifiers to be authorized; in this case, the holder can query the trust registry to determine if the verifier is authorized before sharing any data


rules engine
queries
holder
queries
rules engine
to
presents
credential
pass
publishes rules & queries to qualify holder
issues
queries to verify verifier
to
publishes rules & queries to verify pass
queries to verify issuer
issuer*
verifier
listed in
listed in
trust registry
controls
publishes
governance framework
governing authority
* Original issuer or proxy issuer

Part Four:
The Good Health Pass Ecosystem of Ecosystems

The Good Health Pass digital trust ecosystem does not have just one governing authority— rather it is an ecosystem of ecosystems with many governing authorities

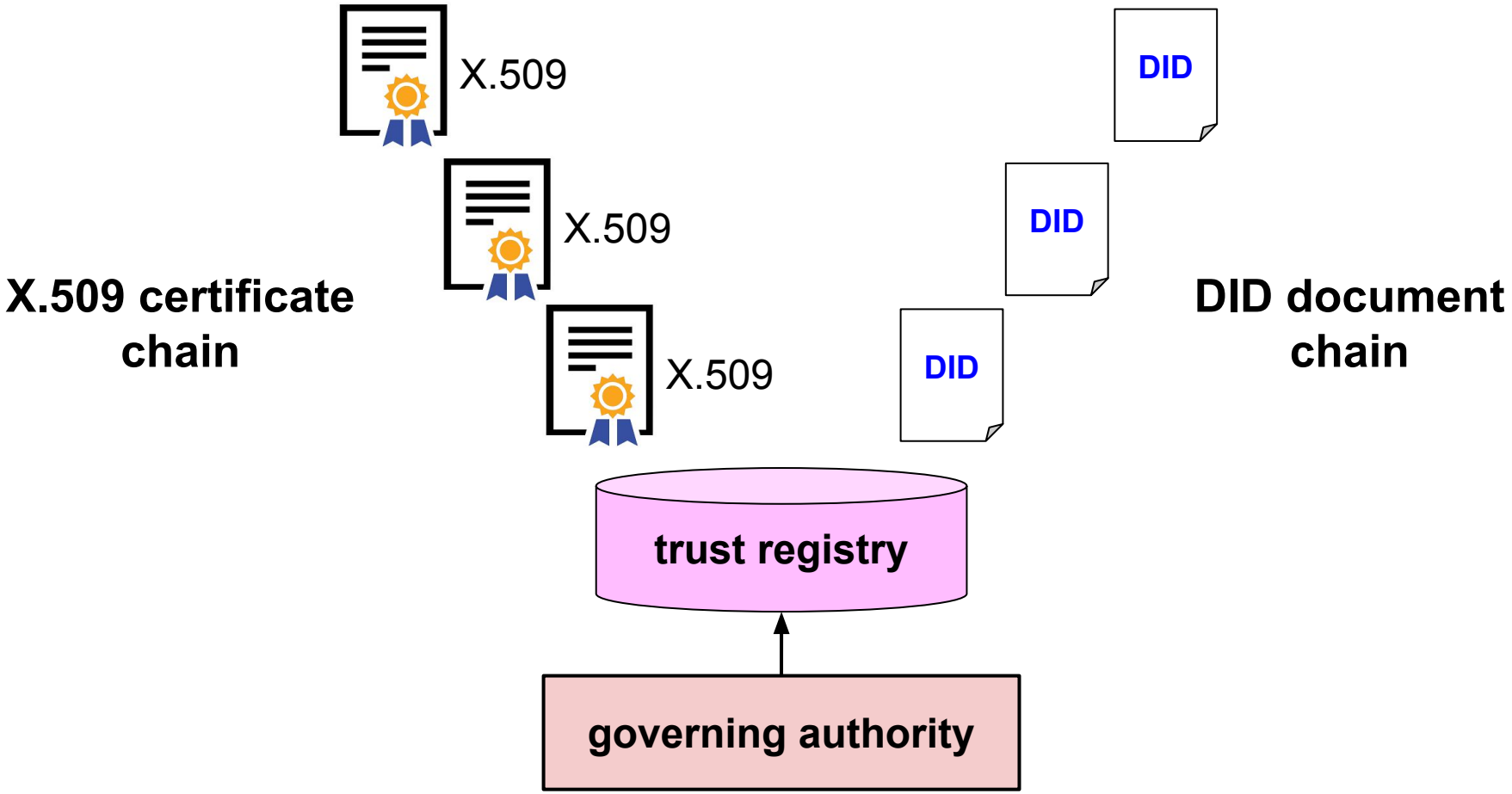
Each governing authority publishes its own governance framework and manages its own trust registry so it serves as its own root of trust


trust registry
governing authority
trust registry
governing authority
trust registry
governing authority
trust registry
governing authority
issue
Holder
present
write
Verifiable Data Registry
read
Issuer
Verifier
trust registry
governing authority
trust registry
governing authority
trust registry
governing authority

Issuers, holders, and verifiers may be part of as many specific ecosystems as needed

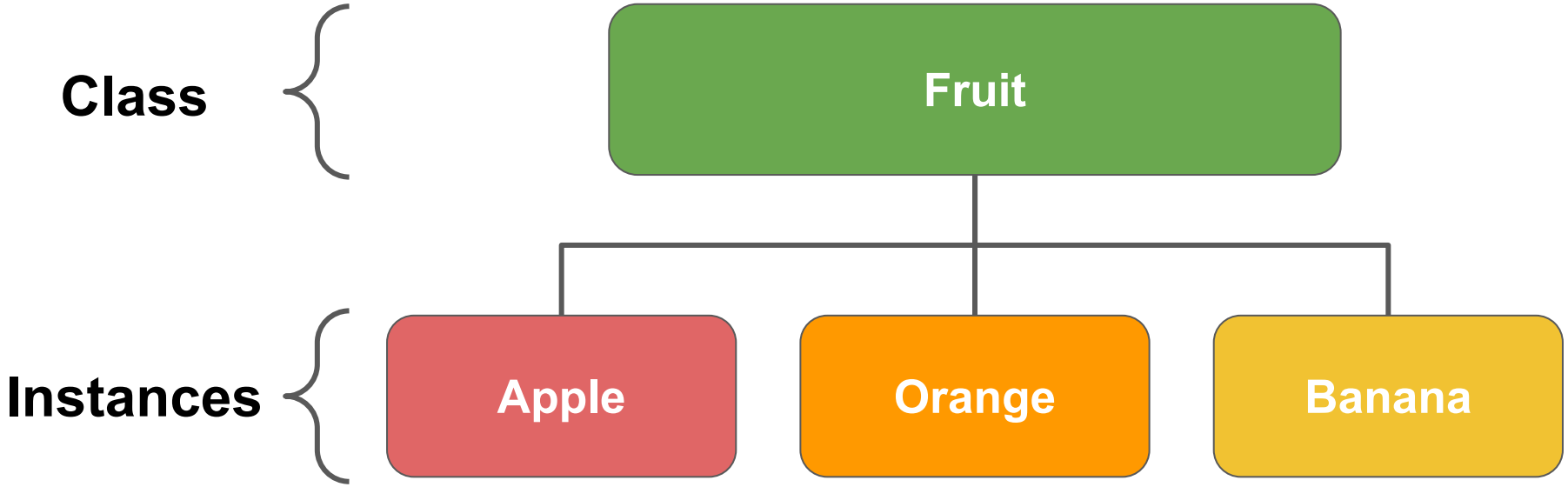
This design enables each governing authority to adapt its ecosystem to its particular jurisdiction, industry, business model, or other specific requirements

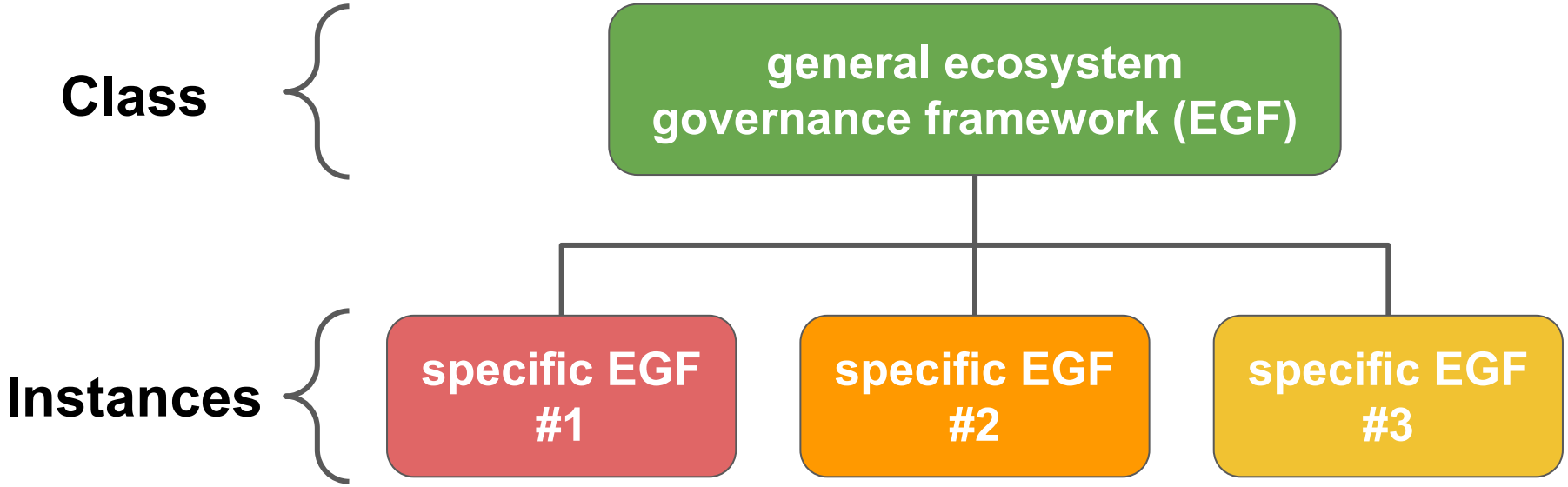
This also enables different ecosystems to use their choice of public key infrastructure (PKI): X.509 public key directories and/or W3C decentralized identifiers (DIDs)

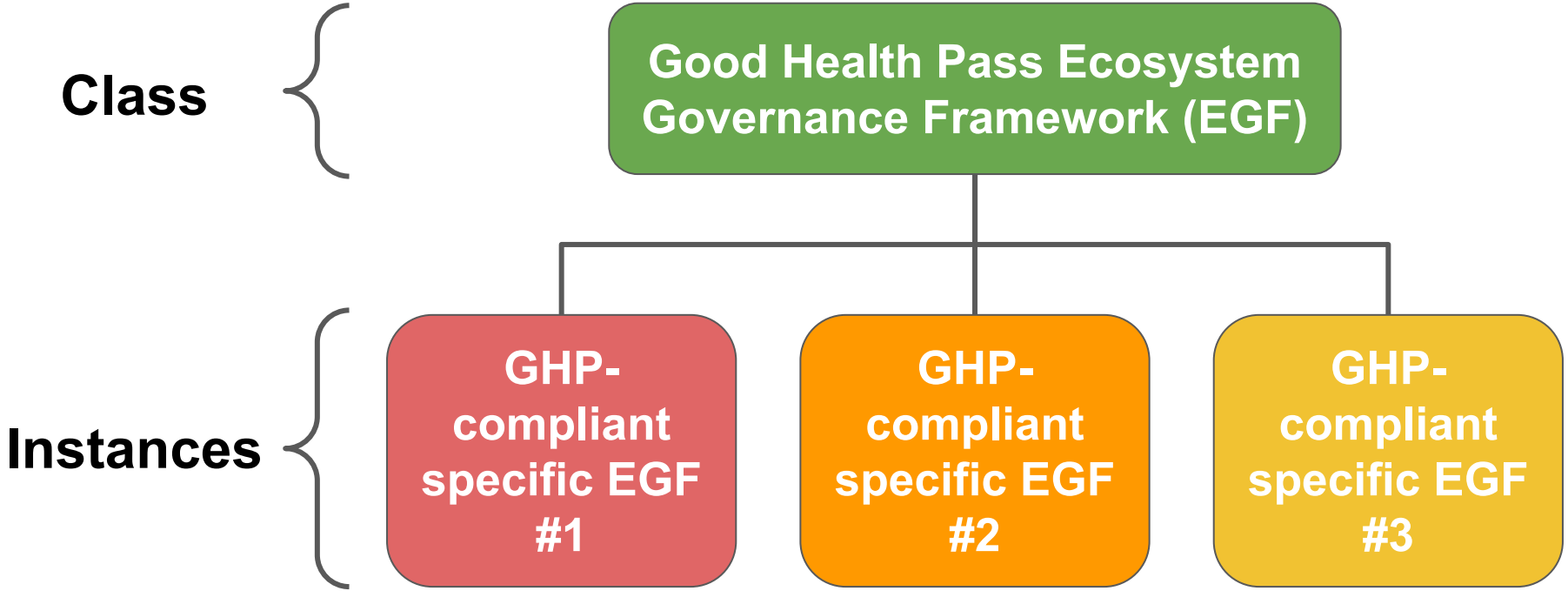

X.509
X.509
X.509
X.509 certificate chain
DID
DID
DID
DID document chain
trust registry
governing authority

What unifies and enables interoperability across the whole ecosystem is the Good Health Pass Ecosystem Governance Framework

It is the class of which all the other specific ecosystem governance frameworks are instances


Class
Fruit
Instances
Apple
Orange
Banana


Class
general ecosystem governance framework (EGF)
Instances
specific EGF #1
specific EGF #2
specific EGF #3


Class
Good Health Pass Ecosystem Governance Framework (EGF)
Instances
GHP-compliant specific EGF #1
GHP-compliant specific EGF #2
GHP-compliant specific EGF #3

This is how we deliver a globally interoperable digital trust ecosystem without requiring a centralized root of trust

For the complete story, please review the
Good Health Pass Interoperability Blueprint