OPEN CREDENTIALING INITIATIVE

Enabling trusted digital interactions
in pharmaceutical supply chains

Agenda

1 **OCI Introduction**

2 **The DSCSA Challenge**

3 **Roadmap**

4 **Appendix**

1 **OCI Introduction**

2 The DSCSA Challenge

3 Roadmap

4 Appendix

What is OCI?

An open **ecosystem** supporting the pharmaceutical industry in complying with **DSCSA** requirements by 2023 with available solutions developed in **industry-wide** pilots

Advantages of OCI Architecture

Every OCI member is committed to adopting and supporting OCI architecture, guidelines, and trust frameworks to support industry collaboration

Efficiency

Verify ATP status instantaneously, with low effort

Interoperability

Share and verify ATP status with any party, with no added friction

Trust

Know-your-ATP through cryptographic resolution and built-in trust

Due diligence

Identify verification carried out in accordance to conformance criteria

Standardization

Global and open standards (GS1 and W3C) ensure no vendor lock-in

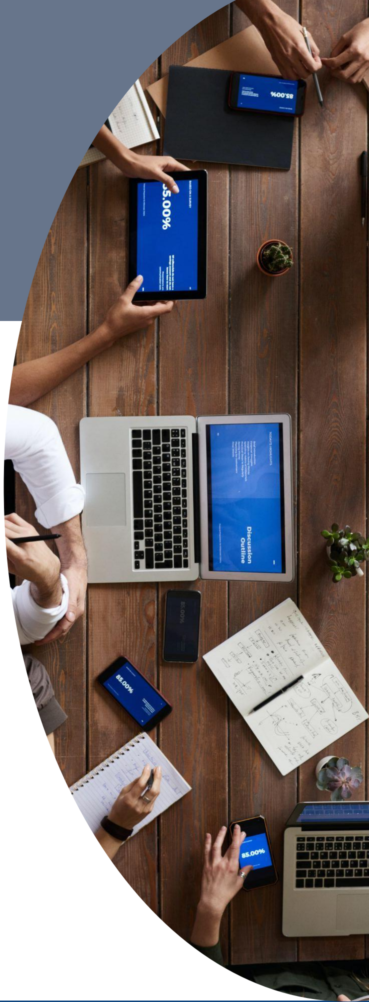
Security-by-design

Protect against fraud and malicious actors

OCI works closely with stakeholders to promote interoperability and DSCSA application

We work with...

- **HDA** to integrate OCI ATP Credentials in PI Verifications processed by VRS
- **GS1 US** to include the optional use of the OCI ATP Header in the GS1 US Guideline for using the Lightweight Messaging Standard for PI Verification
- **PDG** to recognize the OCI architecture as the standard for establishing ATP status in appropriate DSCSA digital transactions
- **AAM** requested to recognize the OCI architecture
- **Trading Partners and Solution Providers** to adopt and onboard
- **FDA** to establish awareness that a solution for the ATP requirement is available and validated by compliance teams

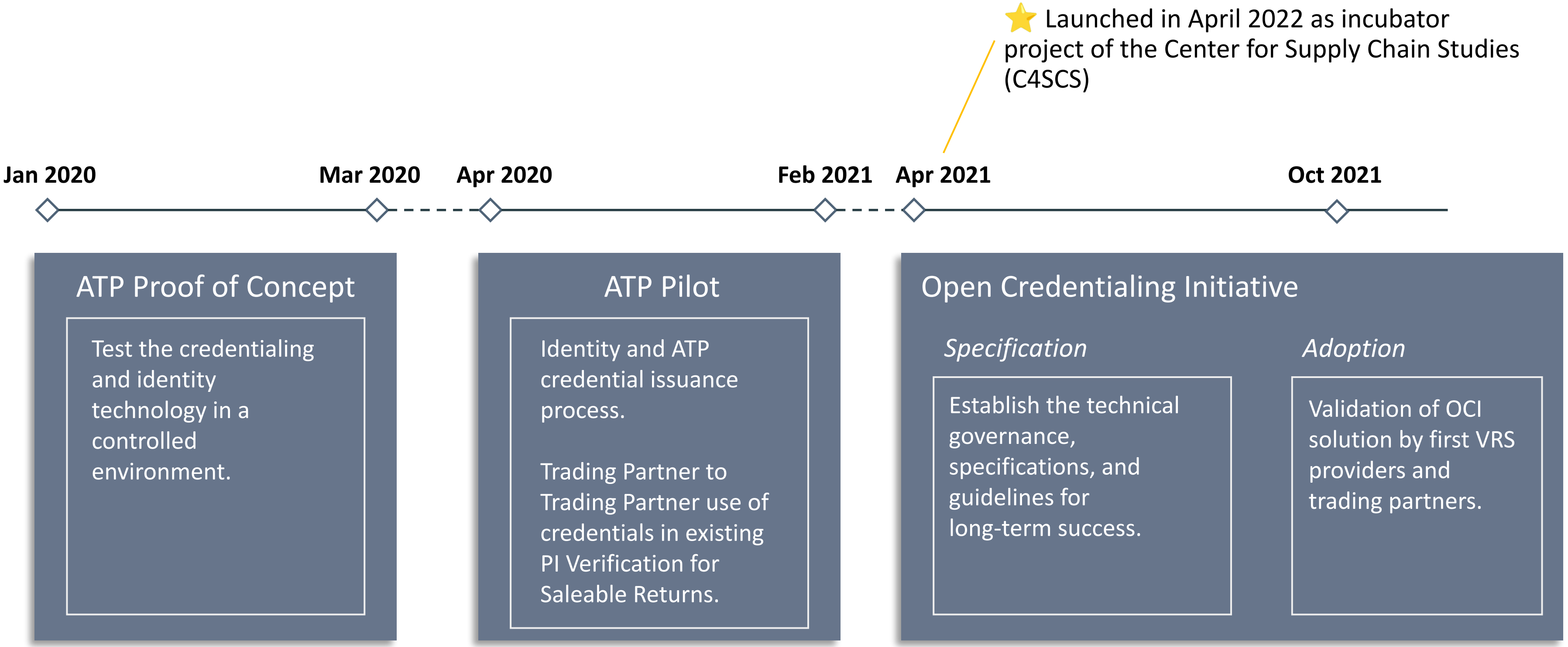


What does the OCI do?

- Incubates **industry-wide adoption** of non-proprietary credentialing solutions
- Defines **conformance and interoperability criteria**
- Coordinates and maintains **frameworks and guidelines** for software architecture
- Applies **open standards** (GS1, W3C and DIF)
- Addresses needs of **all** stakeholders along the pharmaceutical supply chain
- Facilitates pilots to **explore credentialing** for and beyond DSCSA requirements
- **Publication** of all technical work on dedicated GitHub account:

  https://github.com/Open-Credentialing-Initiative

From PoC to OCI



⭐ Launched in April 2022 as incubator project of the Center for Supply Chain Studies (C4SCS)

Jan 2020

Mar 2020

Apr 2020

Feb 2021

Apr 2021

Oct 2021

ATP Proof of Concept

Test the credentialing and identity technology in a controlled environment.

ATP Pilot

Identity and ATP credential issuance process.

Trading Partner to Trading Partner use of credentials in existing PI Verification for Saleable Returns.

Open Credentialing Initiative

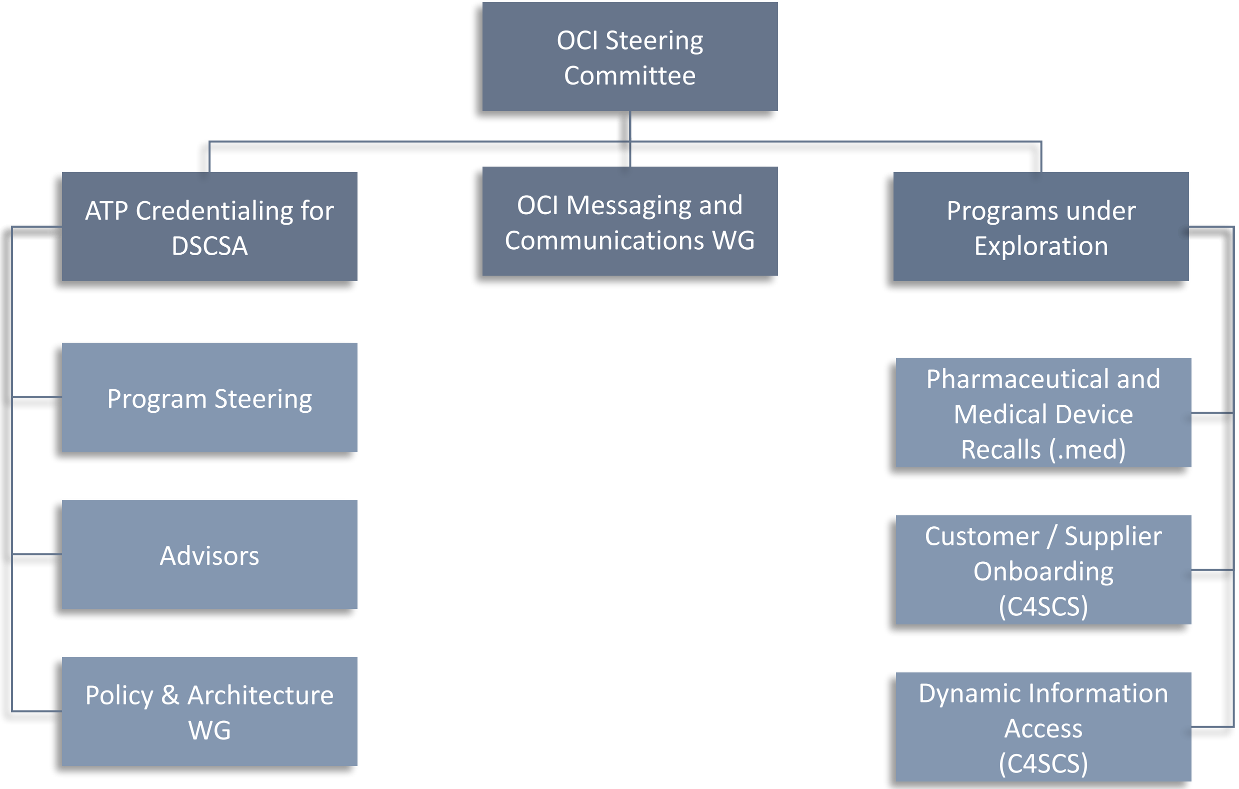
Specification

Establish the technical governance, specifications, and guidelines for long-term success.

Adoption

Validation of OCI solution by first VRS providers and trading partners.

OCI Structure



OCI Steering Committee

ATP Credentialing for DSCSA

OCI Messaging and Communications WG

Programs under Exploration

Program Steering

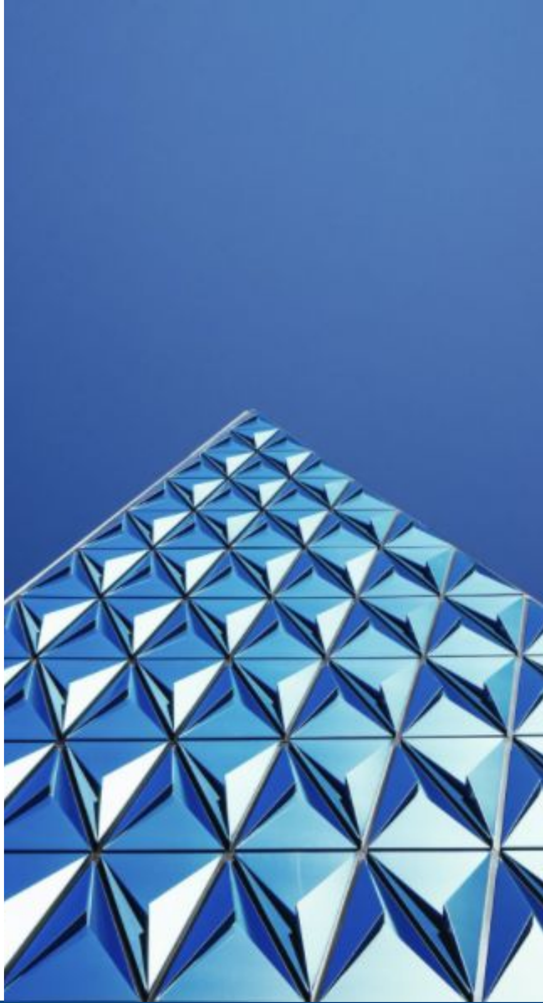
Advisors

Policy & Architecture WG

Pharmaceutical and Medical Device Recalls (.med)

Customer / Supplier Onboarding (C4SCS)

Dynamic Information Access (C4SCS)



The Current OCI Ecosystem

Trading Partners

- Novartis
- Atlantic Biologicals
- Lilly
- Bristol-Myers Squibb*
- Johnson & Johnson*
- AmerisourceBergen*

Integrators

- SAP
- Tracelink
- rfxcel
- RxScan
- Navitas
- .Med

Credential Issuer

- Legisym
- XATP
- .Med

Wallet Provider

- Spherity
- XATP

Supporters

- HDA
- GS1 US

Credential Issuer

- Center for Supply Chain Studies

Early Adopter Program

- Novartis
- Johnson & Johnson
- Bristol-Myers Squibb
- AmerisourceBergen
- Apotex
- Cardinal Health

** Status for committed companies where the legal process to join is pending*

Interested in joining?

Please visit us on oc-i.org and join OCI by signing our charter.

Membership is free for trading partners.

1 OCI Introduction

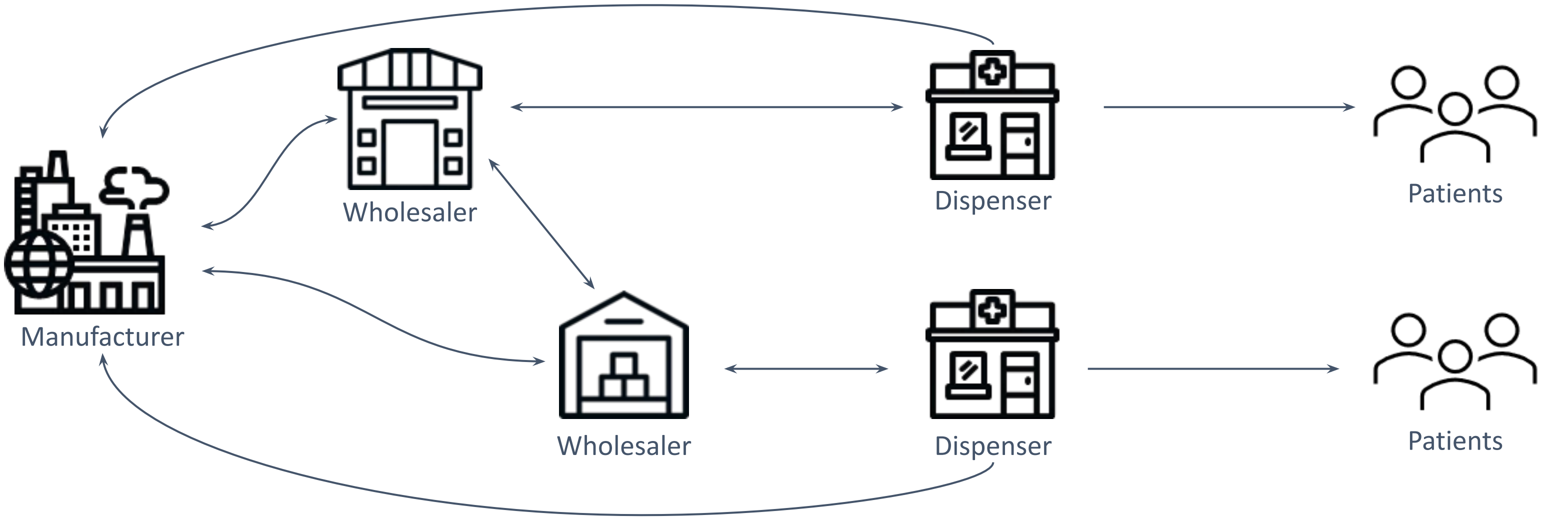
2 **The DSCSA Challenge**

3 Roadmap

4 Appendix

U.S. Drug Supply Chain Security Act (DSCSA)

Securing the drug supply chain all the way by Nov 2023



Prevent harmful drugs from entering the supply chain

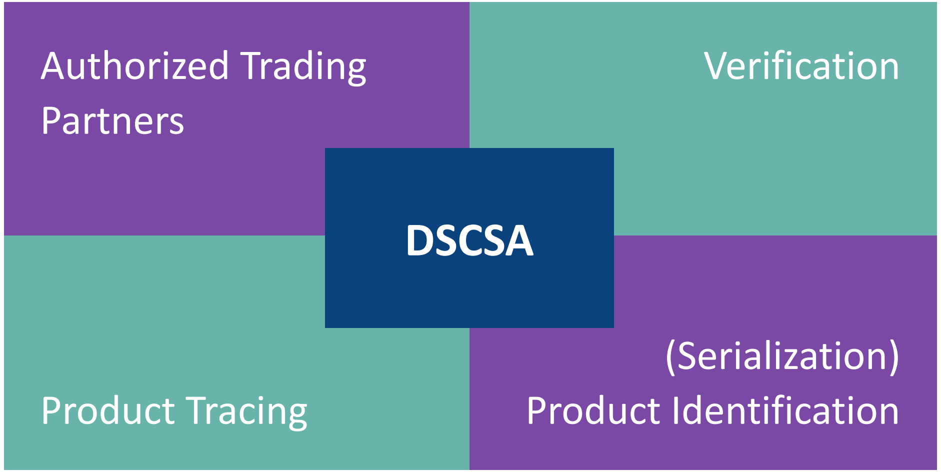
Detect harmful drugs that have entered the supply chain

Respond rapidly when harmful drugs are found

DSCSA states 4 key requirements to be realized by 2023

Key Requirements

(under section 582 of the FD&C Act) apply to Manufacturers, Repackagers, Wholesale Distributors and Dispensers (Pharmacies)



Authorized Trading Partners

Verification

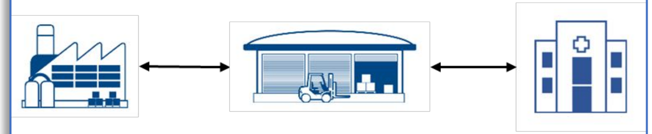
DSCSA

Product Tracing

(Serialization) Product Identification

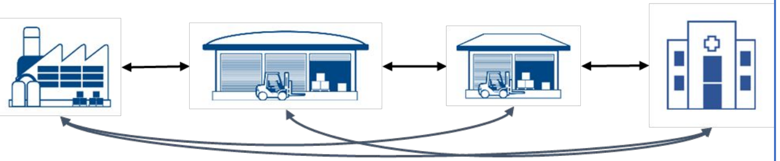
DSCSA requires vetting of indirect Trading Partners

Traditional
“Trading Partner” Relationship



1. Due Diligence (Days?)
2. Individual Digital Connection
   (i.e. AS2)

DSCSA Defined
“Trading Partner” Relationships



Indirect Trading Partner Relationships

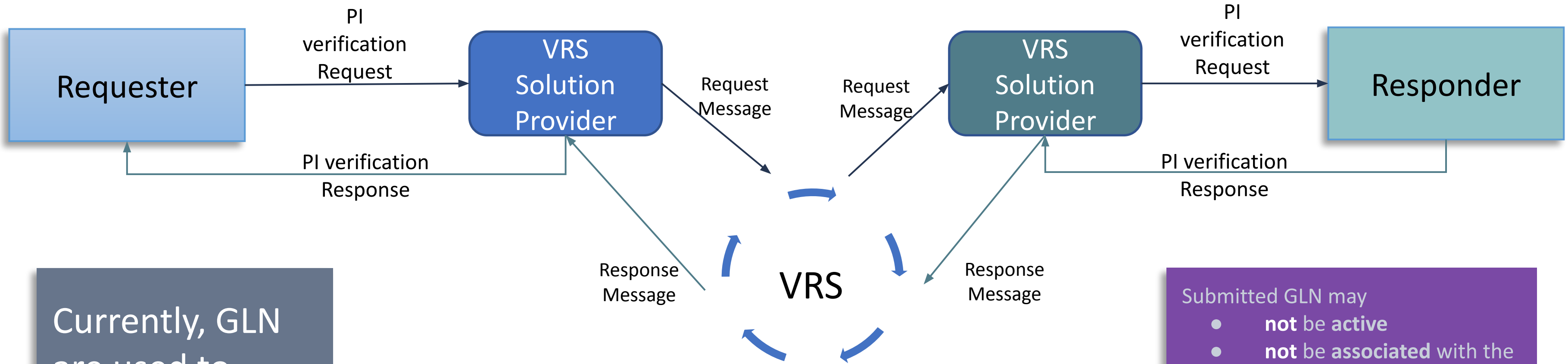
1. Due Diligence (< 1sec)
2. Networked Digital Connections
   (i.e. Verification Routing Service, API)
3. Indirect Trading Partner Relationship
   (< 1sec)

What makes a trading partner authorized?

Entity is a **Trading Partner** when it **accepts or transfers direct ownership** of a product from or to a manufacturer, third-party logistics provider, wholesale distributor or dispenser.

		Entity is Authorized when it ...	Where can Trading Partners check each others authorized status?
Manufacturer	Repackager	Is registered with FDA in accordance with section 510 of the FD&C Act	FDA´s drug establishment current registration database
Wholesale Distributor	Third-Party Logistic Provider	Has a valid state or federal license	Database of authorities
Dispenser, Pharmacy	Clinic	Has a valid license under State law	Database of authorities

GLNs do not suffice to identify trading partners in product identifier verification processes



Requester

PI verification Request

VRS Solution Provider

PI verification Response

Request Message

Response Message

VRS

Request Message

Response Message

VRS Solution Provider

PI verification Request

Responder

PI verification Response

Currently, GLN are used to identify Trading Partners.

Submitted GLN may

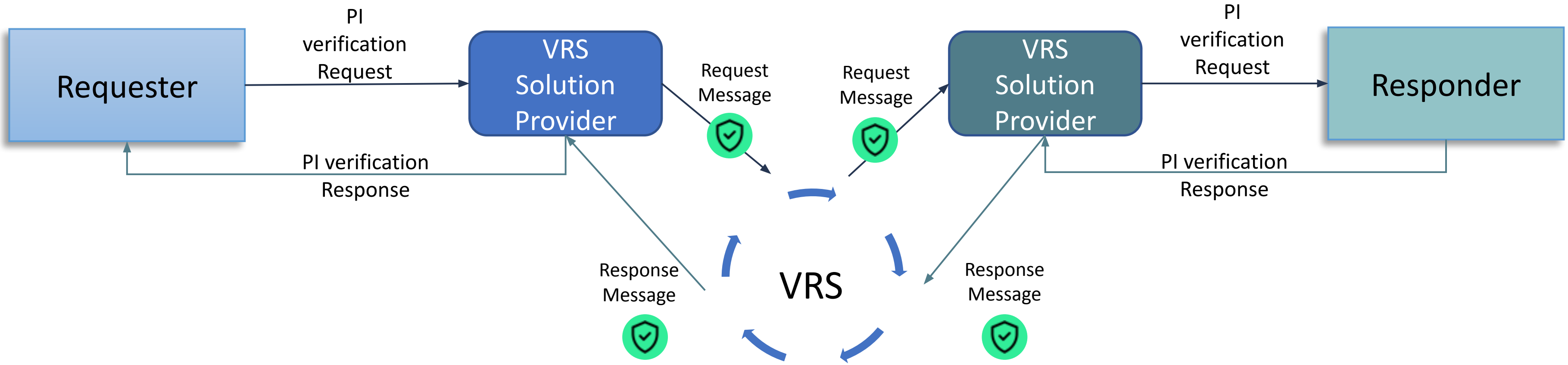
- **not** be **active**
- **not** be **associated** with the Trading Partner

GLN do **not**

- inform about trading **authorization**
- ascertain **origin** of the received GLN

OCI’s ATP Architecture

OCI uses Verifiable Credentials to identify trading partners and verify their authorized status

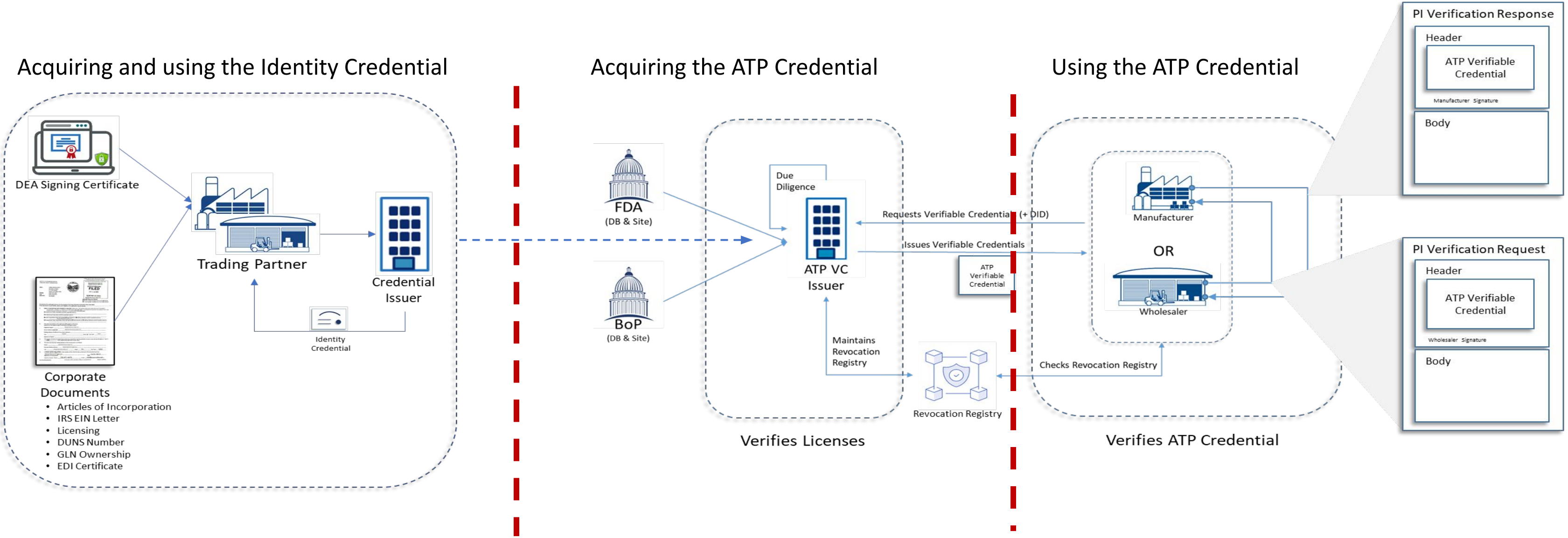


✓ Verifiable Credential

A **credential** is a digital assertion containing a set of claims (e.g., about a state license or FDA Establishment Identifier) made by an entity about itself or another entity. A subset of identity data, credentials are cryptographically signed and can be verified. Credentials can be used to create selective disclosures of information (known as "verifiable presentations") to limit personal data exposure. The entity described by the claims is called the **subject** of the credential.

The OCI uses Verifiable Credentials in accordance with the W3C specification: https://www.w3.org/TR/vc-data-model/

Credentialing introduces cryptographically verifiable trust into the ATP process flow



Acquiring and using the Identity Credential

DEA Signing Certificate

Trading Partner

Credential Issuer

Identity Credential

Corporate Documents

- Articles of Incorporation
- IRS EIN Letter
- Licensing
- DUNS Number
- GLN Ownership
- EDI Certificate

Acquiring the ATP Credential

FDA (DB & Site)

BoP (DB & Site)

Due Diligence

ATP VC Issuer

Maintains Revocation Registry

Revocation Registry

Verifies Licenses

Requests Verifiable Credential (+ DID)

Issues Verifiable Credentials

ATP Verifiable Credential

Using the ATP Credential

Manufacturer

OR

Wholesaler

Checks Revocation Registry

Verifies ATP Credential

PI Verification Response

Header

ATP Verifiable Credential

Manufacturer Signature

Body

PI Verification Request

Header

ATP Verifiable Credential

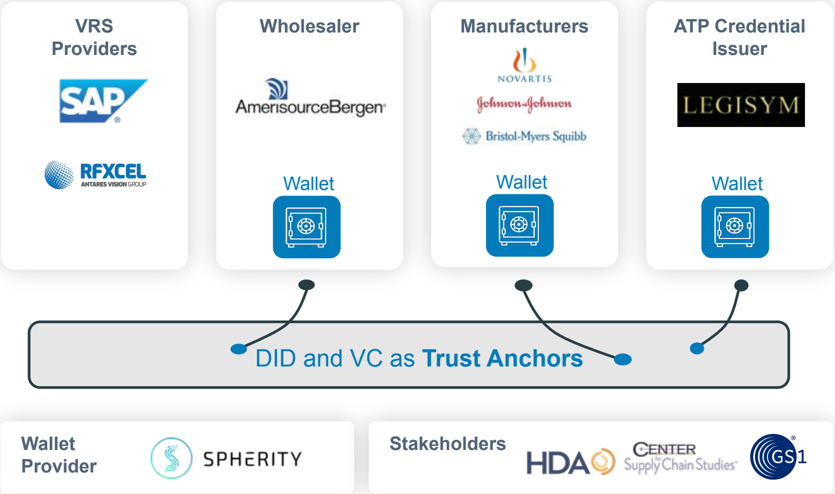
Wholesaler Signature

Body

Start of cryptographically verifiable trust

Trading Partner cryptographically verifiable trust

ATP Pilot proved feasibility using Credentials in product verifications



VRS Providers

Wholesaler

Wallet

Manufacturers

Wallet

ATP Credential Issuer

Wallet

DID and VC as **Trust Anchors**

Wallet Provider

Stakeholders

Info Material

Explainer Videos

Link

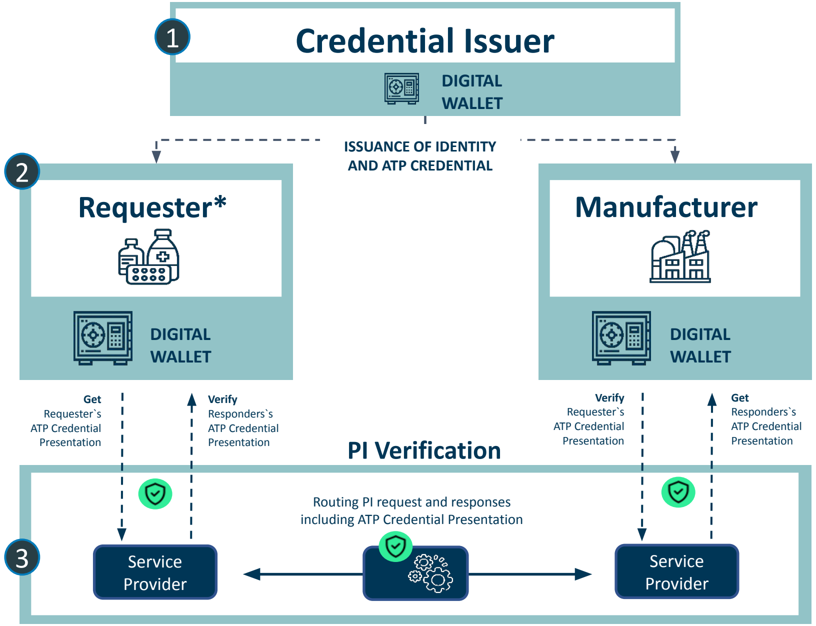
Pilot Resources

Link

Main Results

- **Scalable, interoperable** technology
- **Compliant with DSCSA** ATP requirements
- Credentialing can be **integrated into existing processes with little effort**
- **No update of GS1** standard required
- Continued **collaboration** within OCI to drive **adoption** of credentialing

Architecture for PI Verification using Credentials to check ATP status


1
Credential Issuer
DIGITAL WALLET
ISSUANCE OF IDENTITY AND ATP CREDENTIAL
2
Requester*
DIGITAL WALLET
Manufacturer
DIGITAL WALLET
Get Requester`s ATP Credential Presentation
Verify Responders`s ATP Credential Presentation
Verify Requester`s ATP Credential Presentation
Get Responders`s ATP Credential Presentation
PI Verification
Routing PI request and responses including ATP Credential Presentation
3
Service Provider
Service Provider

*) Wholesaler, dispenser, clinic…

Details

1

- OCI-conformant credential issuer **verifies organization's identity and license status**
- Establishes digital link between organization and digital identifier (DID) by issuing an **identity credential**
- **Usage of Digital Wallet** and registration of own identifier (DID) in public registry
- Verifies authorized status and issues **ATP credential**

2

- Trading partner provides credential issuer information to be identified as **legitimate organization and authorized trading partner**
- **Usage of digital wallet** to acquire, present and verify credentials
- Provides VRS API access to digital wallet to allow the creation of credential presentations and verifications
- **Digital wallet logs** all credential presentations and verification **transactions**

3

- VRS uses OCI **open APIs** to interact with digital wallet of own customer
- **Creates ATP credential presentation via API** and attaches it to GS1-standardized request or response message
- **Verifies ATP credential presentation** sent to customer

OCI conformance criteria enable interoperability

Trading Partners

- Novartis
- Atlantic Biologicals
- Lilly
- Bristol-Myers Squibb*
- Johnson & Johnson*
- AmerisourceBergen*

Integrators

- SAP
- Tracelink
- rfxcel
- RxScan
- Navitas
- .Med

Credential Issuer

- Legisym
- XATP
- .Med

Wallet Provider

- Spherity
- XATP

Supporters

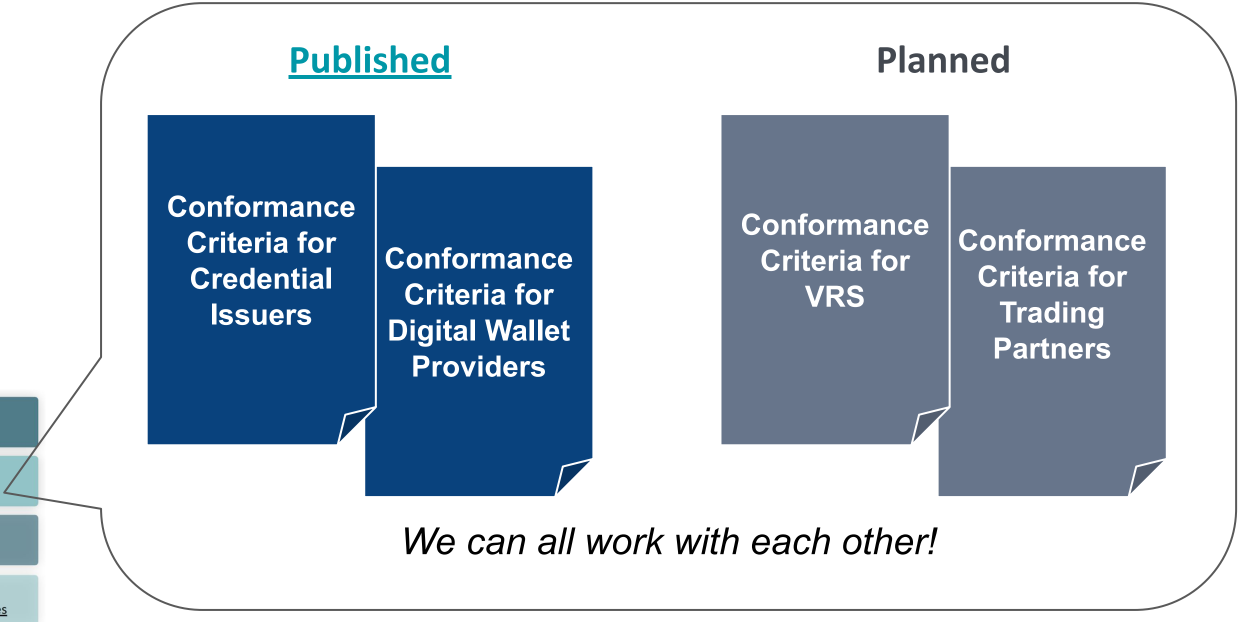
- HDA
- GS1 US

Observer

- Center for Supply Chain Studies

Early Adopter Program

- Novartis
- Johnson & Johnson
- Bristol-Myers Squibb
- AmerisourceBergen
- Apotex
- Cardinal Health



Published

Conformance Criteria for Credential Issuers

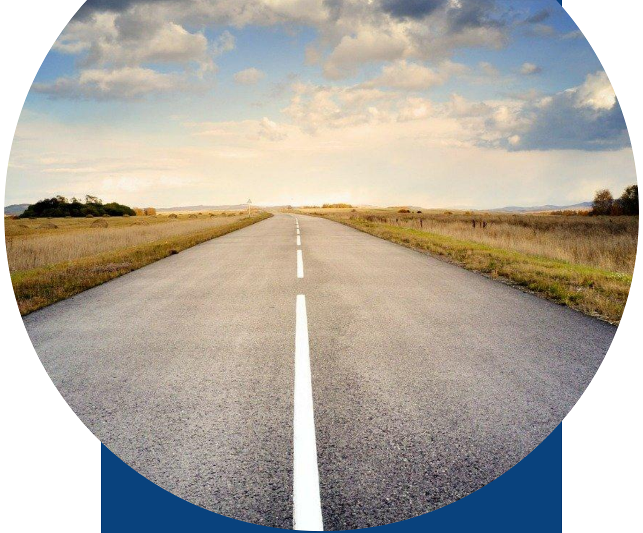
Conformance Criteria for Digital Wallet Providers

Planned

Conformance Criteria for VRS

Conformance Criteria for Trading Partners

We can all work with each other!



1 OCI Introduction

2 The DSCSA Challenge

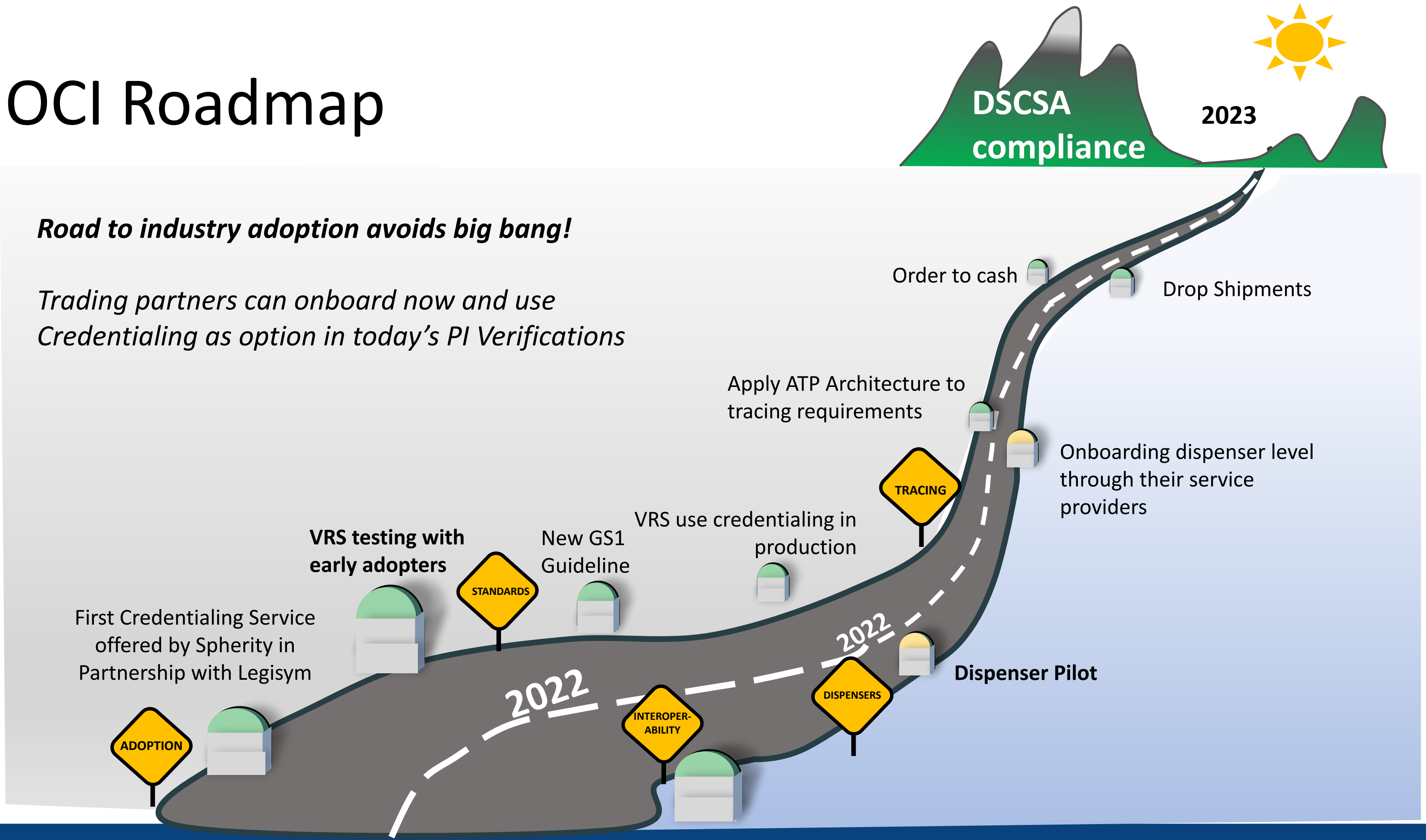
3 **Roadmap**

4 Appendix

OCI Roadmap

Road to industry adoption avoids big bang!

Trading partners can onboard now and use Credentialing as option in today's PI Verifications



DSCSA compliance
2023
Order to cash
Drop Shipments
Apply ATP Architecture to tracing requirements
Onboarding dispenser level through their service providers
TRACING
VRS use credentialing in production
New GS1 Guideline
VRS testing with early adopters
STANDARDS
First Credentialing Service offered by Spherity in Partnership with Legisym
ADOPTION
2022
INTEROPER-ABILITY
2022
DISPENSERS
Dispenser Pilot

Get involved

- ❑ **Test drive** OCI’s solution by joining the current validation cycle. Register your interest!
- ❑ **Join** OCI
- ❑ **Educate** your teams
- ❑ **Participate** at future events
- ❑ Contact us at **hello@oc-i.org**

1 OCI Introduction

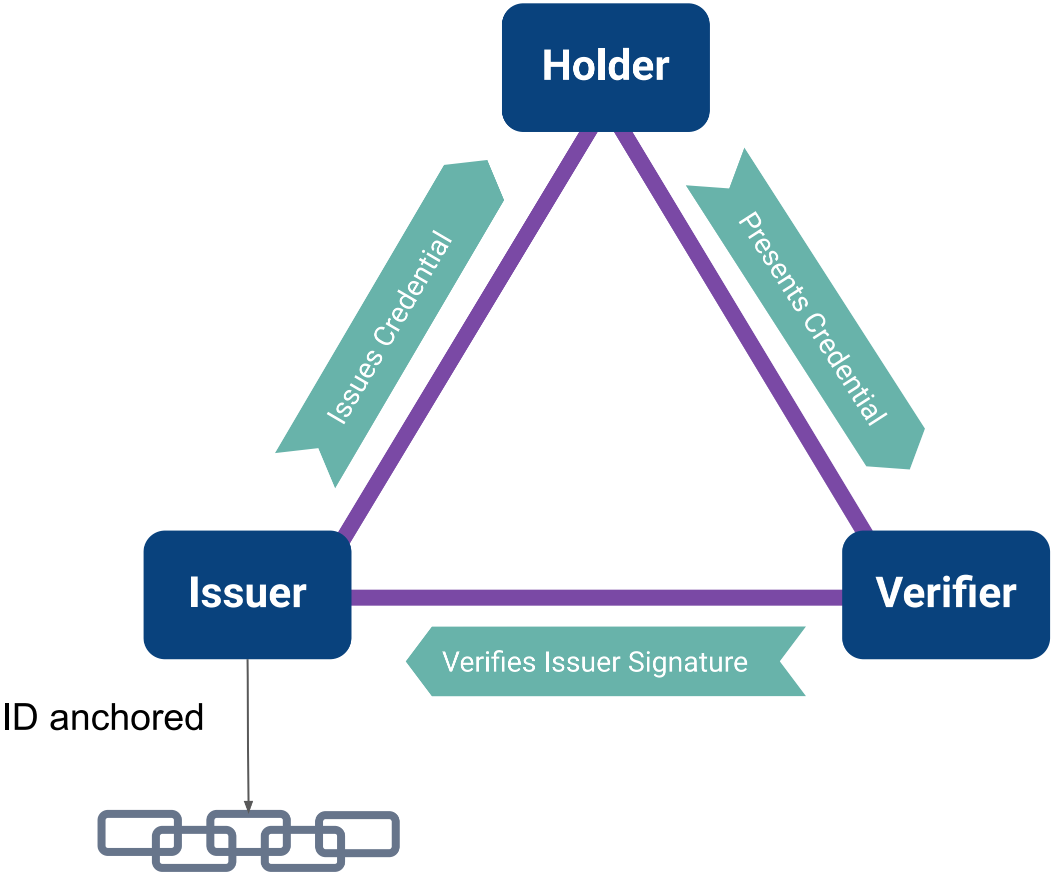
2 The DSCSA Challenge

3 Roadmap

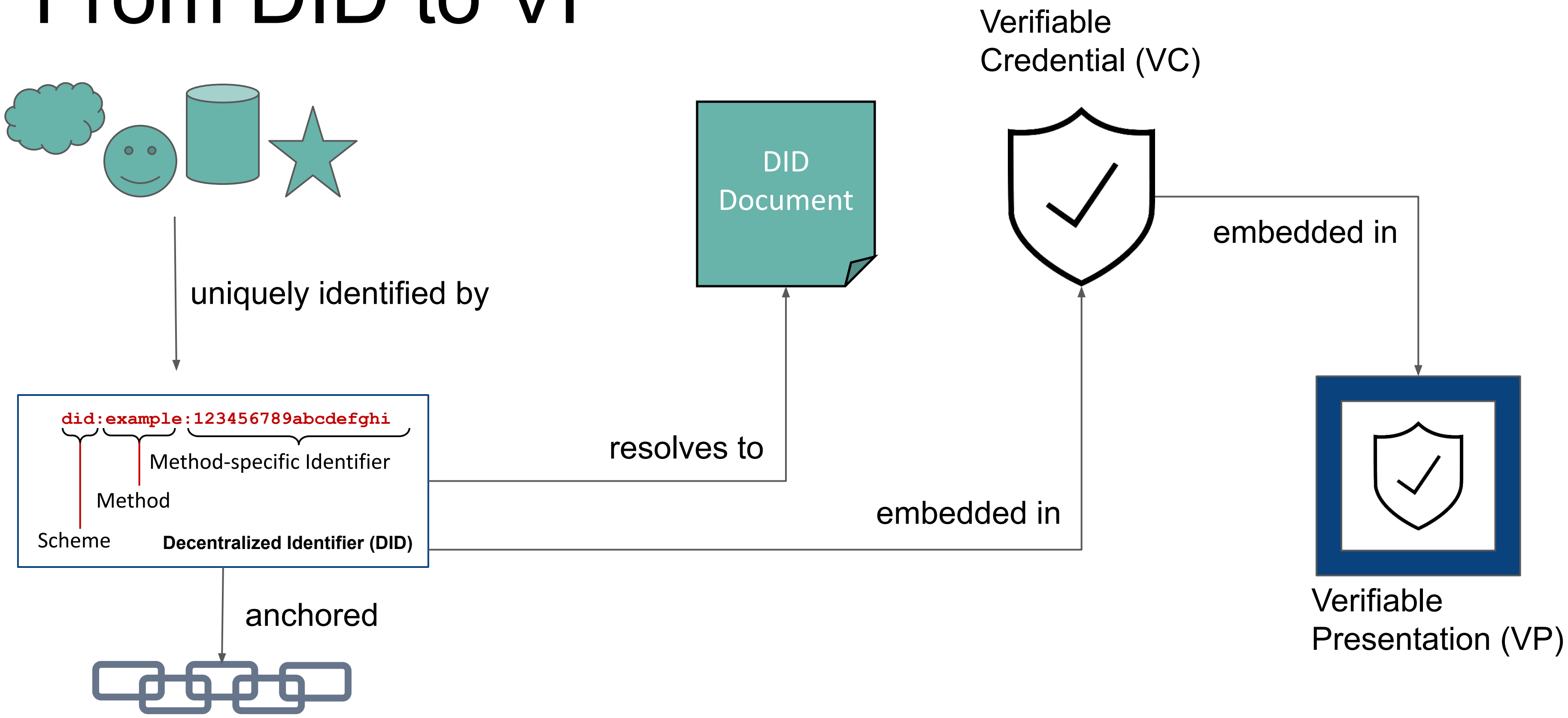
4 **Appendix**

Background on credentials

Trust triangle



From DID to VP


Verifiable Credential (VC)
DID Document
uniquely identified by
embedded in
did:example:123456789abcdefghi
Method-specific Identifier
Method
Scheme
Decentralized Identifier (DID)
resolves to
embedded in
anchored
Verifiable Presentation (VP)

DID, DID Doc, VC

Decentralized Identifier (DID)

is a new type of identifier that is globally unique, resolvable with high availability, and cryptographically verifiable. DIDs are typically associated with cryptographic material, such as public keys, and service endpoints, for establishing secure communication channels.

DID Document (DID Doc)

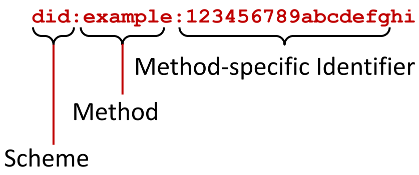
contains metadata about the DID subject (entity, person, thing). Contains minimum amount of information needed to establish a trustable connections with the DID subject.

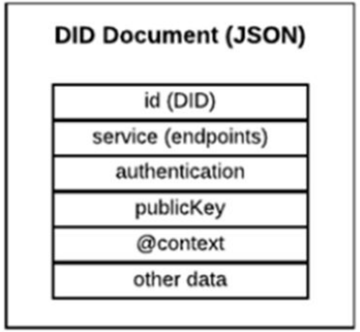
- Public key (needed for encrypted and authenticated communication)
- Service endpoints (where the subject's API is)
- Authentication Methods
- Timestamps, proofs
- Other identifier metadata

DID document is completely public

Verifiable Credential (VC)

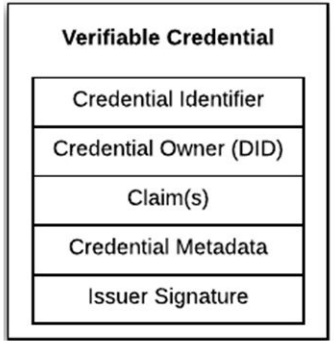
is a piece of information that is cryptographically trustworthy. It is shared as a proof and is anchored to a public ledger by a **credential** definition and public DID written by the **credential** issuer.





DID Document (JSON)

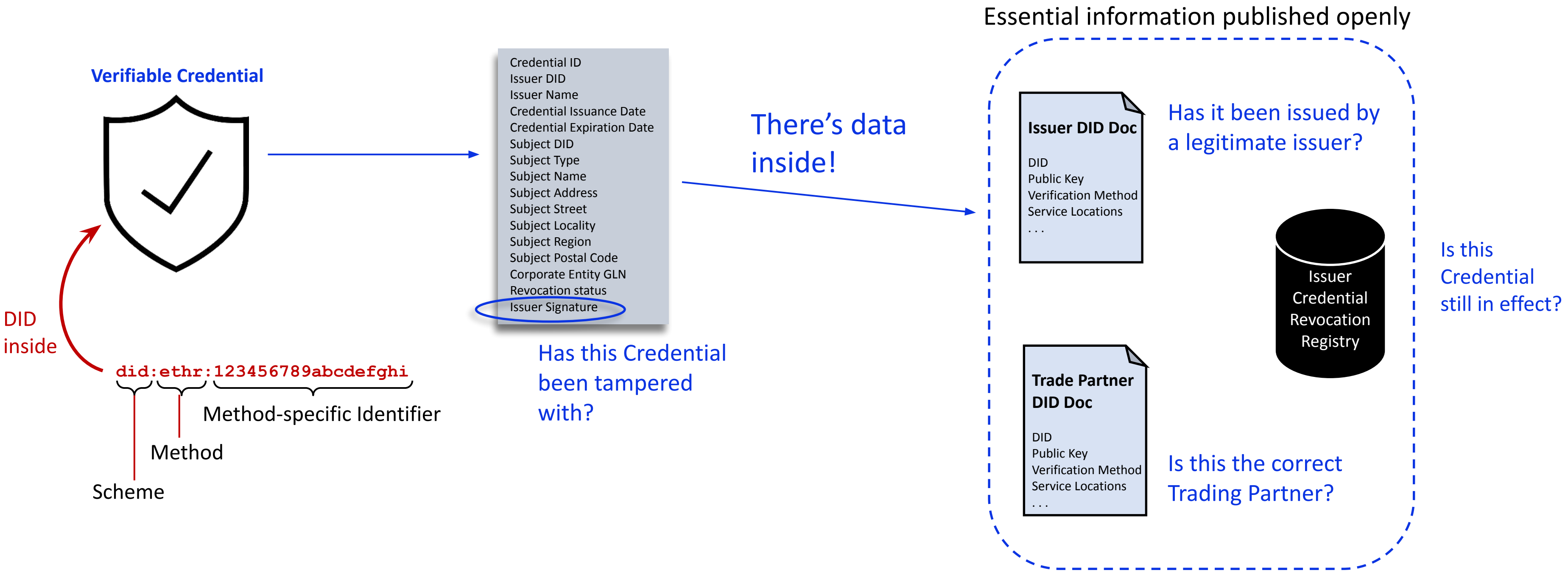
id (DID)
service (endpoints)
authentication
publicKey
@context
other data



Verifiable Credential

Credential Identifier
Credential Owner (DID)
Claim(s)
Credential Metadata
Issuer Signature

Relationship between DID and VC



Verifiable Credential

Credential ID
Issuer DID
Issuer Name
Credential Issuance Date
Credential Expiration Date
Subject DID
Subject Type
Subject Name
Subject Address
Subject Street
Subject Locality
Subject Region
Subject Postal Code
Corporate Entity GLN
Revocation status
Issuer Signature

DID inside

did:ethr:123456789abcdefghi

Scheme

Method

Method-specific Identifier

Has this Credential been tampered with?

There's data inside!

Essential information published openly

Issuer DID Doc

DID
Public Key
Verification Method
Service Locations
. . .

Has it been issued by a legitimate issuer?

Issuer Credential Revocation Registry

Is this Credential still in effect?

Trade Partner DID Doc

DID
Public Key
Verification Method
Service Locations
. . .

Is this the correct Trading Partner?

Credential Schema support interoperability

Schemas are the general structure of the credential.

Identity Credential

Within the OCI ecosystem, the Identity Credential is the Root of Trust upon which issuance of ATP Credentials depends. The due diligence expected of the Credential Issuer is established by OCI, and this due diligence must be exercised prior to issuing an Identity Credential.

```
{
  "@context": {
    "@version": 1.1,
    "@protected": true,

    "IdentityCredential": {
      "@id": "https://example.org#IdentityCredential-v2.0.0",
      "@context": {
        "@version": 1.1,
        "@protected": true,
        "id": "@id",
        "type": "@type",
        "schema": "http://schema.org/",

        "issuerName": "schema:legalName",
        "legalName": "schema:legalName",
        "parentOrganization": "schema:parentOrganization",
        "streetAddress": "schema:streetAddress",
        "addressLocality": "schema:addressLocality",
        "addressRegion": "schema:addressRegion",
        "postalCode": "schema:postalCode",
        "addressCountry": "schema:addressCountry"
      }
    }
  }
}
```

ATP Credential

The Credential Issuer performs due diligence on the license status of the trading partner and issue an ATP credential if appropriate.

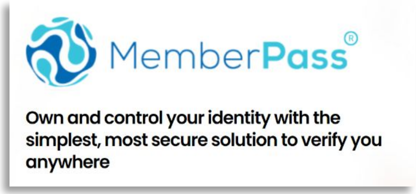
```
{
  "@context": {
    "@version": 1.1,
    "@protected": true,

    "DSCSAATPCredential": {
      "@id": "https://example.org#DSCSAATPCredential-v2.0.0",
      "@context": {
        "@version": 1.1,
        "@protected": true,
        "id": "@id",
        "type": "@type",
        "schema": "http://schema.org/",

        "organizationType": {
          "@id": "schema:additionalType",
          "@type": "schema:additionalType"
        },
        "identifier": {
          "@id": "schema:PropertyValue",
          "@type": "schema:PropertyValue"
        },
        "issuerName": "schema:legalName",
        "legalName": "schema:legalName",
        "streetAddress": "schema:streetAddress",
        "addressLocality": "schema:addressLocality",
        "addressRegion": "schema:addressRegion",
        "postalCode": "schema:postalCode",
        "addressCountry": "schema:addressCountry"
      }
    }
  }
}
```

Link to OCI schemas:
https://github.com/Open-Credentialing-Initiative/schemas

Where else are W3C Standard Verifiable Credentials used?

Pan-Canadian Trust Framework™

Connecting Canadians and Canadian Companies to Government Services.



MemberPass®

Own and control your identity with the simplest, most secure solution to verify you anywhere

Identity credentials allowing Customers to access services from any Credit Union.

Homeland Security

Silicon Valley Innovation Program (accelerate tech. transition) / Digital identity
Start: 09/19
10 SME awarded

PharmaLedger

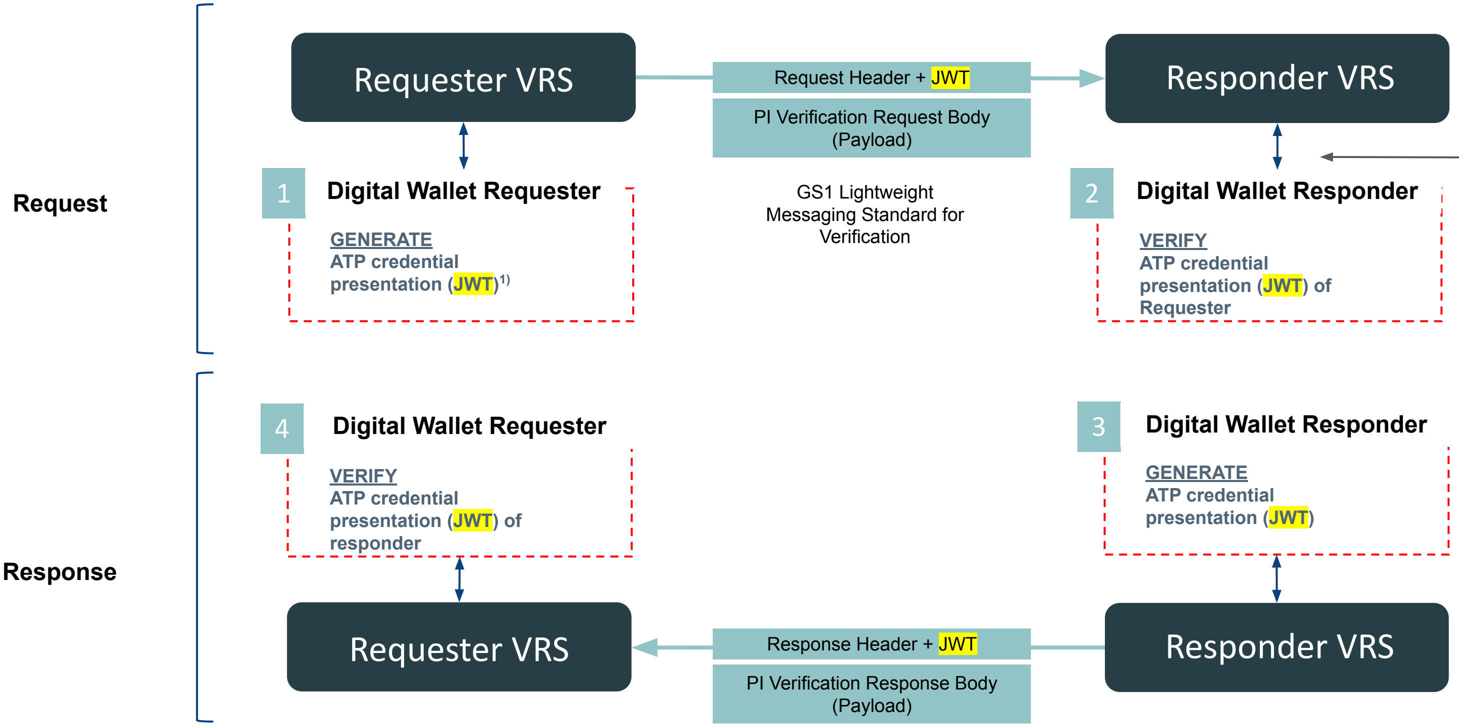
Blockchain Platform for pharma supply chain, clinical trials
Start: 01/20
Novartis, AstraZeneca, Bayer, Roche, Pfizer, others

NCR

NCR's next-generation retail store architecture.

OCI Technology Architecture

Detailed PI Verification roundtrip with OCI



Request

Requester VRS

Request Header + JWT

PI Verification Request Body (Payload)

Responder VRS

1 Digital Wallet Requester

GENERATE ATP credential presentation (JWT)[1)]

GS1 Lightweight Messaging Standard for Verification

2 Digital Wallet Responder

VERIFY ATP credential presentation (JWT) of Requester

Response

4 Digital Wallet Requester

VERIFY ATP credential presentation (JWT) of responder

3 Digital Wallet Responder

GENERATE ATP credential presentation (JWT)

Requester VRS

Response Header + JWT

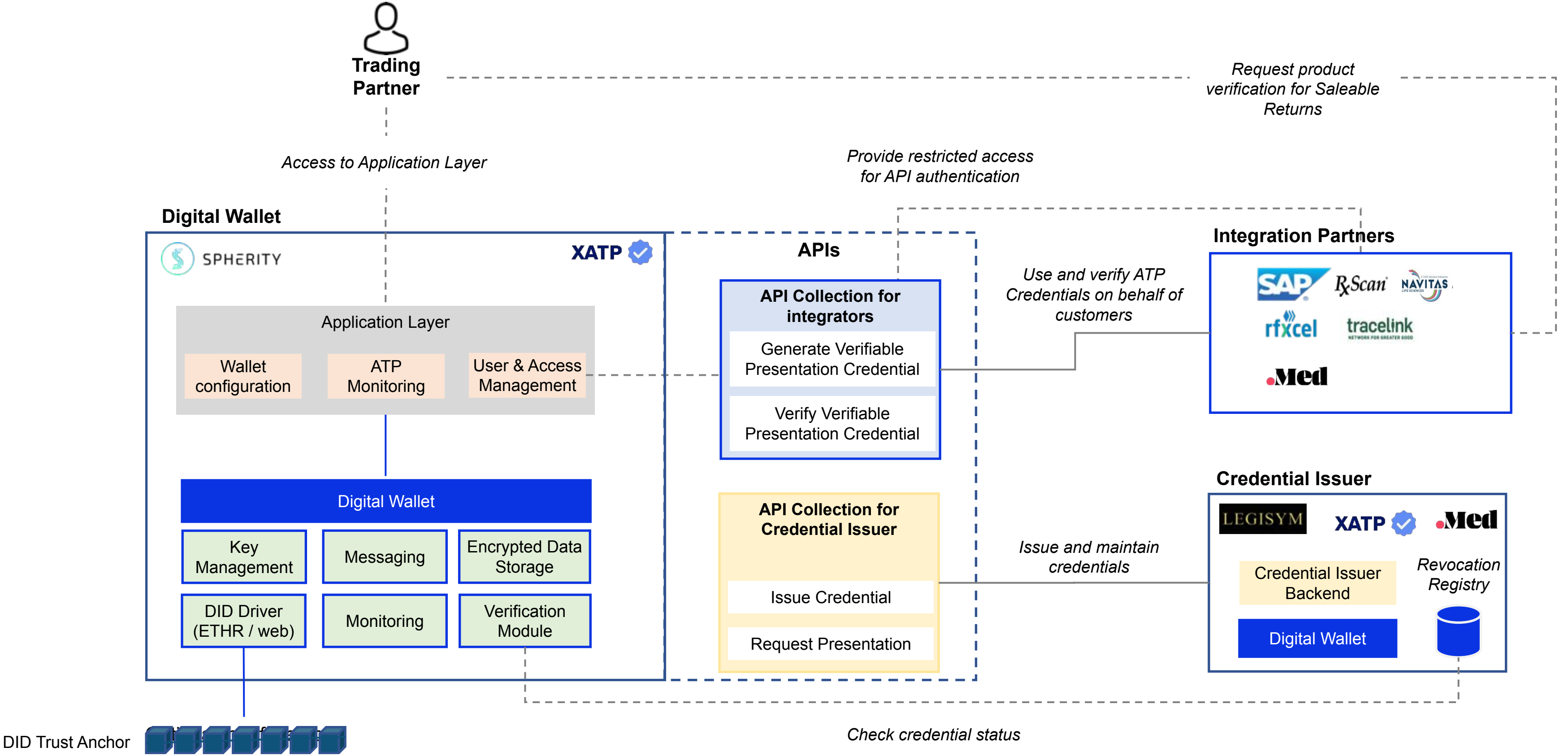
PI Verification Response Body (Payload)

Responder VRS

Open APIs for VRS providers specified by OCI here.

1) JSON Web Token - OCI uses JWT for wrapping credentials into a verifiable presentation. Used specification: https://w3c.github.io/vc-data-model/#jwt-encoding

OCI System Architecture with Ecosystem Partners


Trading Partner
Request product verification for Saleable Returns
Access to Application Layer
Provide restricted access for API authentication
Digital Wallet
SPHERITY
XATP
Application Layer
Wallet configuration
ATP Monitoring
User & Access Management
Digital Wallet
Key Management
Messaging
Encrypted Data Storage
DID Driver (ETHR / web)
Monitoring
Verification Module
APIs
API Collection for integrators
Generate Verifiable Presentation Credential
Verify Verifiable Presentation Credential
API Collection for Credential Issuer
Issue Credential
Request Presentation
Use and verify ATP Credentials on behalf of customers
Integration Partners
SAP
RxScan
NAVITAS
rfxcel
tracelink
.Med
Issue and maintain credentials
Credential Issuer
LEGISYM
XATP
.Med
Credential Issuer Backend
Revocation Registry
Digital Wallet
Check credential status
DID Trust Anchor