Center for Supply Chain Studies

Credentialized ATP Pilot

Utilizing Verifiable Credentials to establish **A**uthorized **T**rading **P**artner Status
Supporting Drug Supply Chain Security Act (DSCSA) compliance
PUBLIC REPORT

ATP Pilot Report
Final v01
3-12-2021

Contents

Document Updates

Version	Date	Update
0.01	3/12/2021	First Published Version

Purpose of this Document

This document is for pilot participants only. After editing is complete on this document, the team will decide if anything in this document should not be published in the public version of this Pilot Report.

This document is to provide a high-level overview of the ATP Pilot. The pilot also produced an explainer video and step through demo which provide an easy-to-understand walkthrough of the issue faced by the US Pharmaceutical supply chain community and the approach of the piloted solution.[1]

The Pilot team also created companion documents which provide further detail into the compliance, business operations and technical aspects of the pilot architecture. They are published as part of this pilot:

- ATP Pilot User Journey
- Architecture Handbook
- ATP Credentialing - Audit Requirements
- ATP Credentialing Pilot – Security Analysis
- Identity Wallet API Documentation
- Explainer video
- Step through demo

[1] The pilot explainer video and step-through demo are available on the Center's website: https://www.c4scs.org/atp-pilot

Executive Summary

In April of 2020, companies representing all segments of the US pharmaceutical supply chain, solution providers, a key industry association, and a standards body formed a cross-functional team to pilot the use of Decentralized Identifiers and Verifiable Credentials to establish Drug Supply Chain Security Act (DSCSA) defined "Authorized Trading Partner" status of trading partners involved in automated Product Information Verifications for saleable returns. The pilot successfully concluded in February 2021.

The pilot had been preceded by a proof of concept (PoC) performed by Novartis, SAP, and Spherity who had performed a successful limited test of the W3C standards-based technologies. This pilot expanded on the PoC by adding additional trading partners and solution providers, and proving the technology could effectively be used between manufacturers and wholesalers representing both direct and indirect trading partners supported by separate Verification Routing Service solutions.

While the pilot was initiated to test the use of credential-enhanced PI Verification messages between separate VRS solutions, it ultimately demonstrated[2]:

- Agreed (consensus) roles and responsibilities of stakeholders.
- Due Diligence necessary of credential Issuers.
- Enforcement of compartmentalized access to signing capabilities and private keys.
- An architecture that makes use of the existing VRS solution.
- The use and role of Decentralized Identifiers, Verifiable Credentials and Verifiable Presentations
- Audit records necessary to support audits and investigations.
- The trustworthiness of the whole to safely allow digital interactions between previously unknown companies.

Although manufacturers, wholesalers, and dispensers currently establish the authorized trading partner status of direct trading partners (those that they directly purchase from or sell to), there are a number of DSCSA required interactions between companies where a direct trading partner relationship has not been established (see Figure 1). In these "indirect" interactions, trading partners are still bound by the DSCSA to establish that the other trading partner holds authorized trading partner status. Product Information (PI) Verification[3] is one of those DSCSA required interactions. Specifically, this pilot focused on PI Verifications for saleable returns.[4] The team asserts that this same technology can be used to establish DSCSA defined authorized trading partner status of companies involved in other DSCSA required interactions such as PI Verification for investigations.[5] The pilot successfully integrated a suite of processes necessary to incorporate proper due diligence in first establishing the digital identity of a trading partner, establishing their authorized trading partner status, exchanging proof of ATP status in PI Verification interactions, and cryptographically verifying that proof. The pilot also successfully demonstrated that trading partners alone were able to control their digital identity with secured private keys, could grant limited use of their credentials to their VRS provider, and that proper audit records of

[2] see Key Components of the Piloted Solution

[3] PI Verification is the process of a manufacturer verifying that a drug package with a specific NDC, Serial Number, Lot Number and Expiration Date was placed into commerce.

[4] Saleable returns - products returned to a wholesaler who then deems that the product is in saleable condition.

[5] PI Verification for investigations – an interaction involving manufacturers and wholesalers and also manufacturers and dispensers.

ATP interactions were created. For investigations, audit trails are documented and kept at each point by the trading partners, VRS Providers, Digital Identity Wallets, and Verifiable Credential Issuers.

Once each participant was comfortable with the cryptographic security of using Decentralized Identifiers and Verifiable Credentials, and was briefed on the use of the underlying technology and the processes necessary to establish, maintain and use credentials, the VRS providers found the architecture straightforward to integrate and the trading partners found the process straightforward and easy to follow and understand.

The pilot established that the combination of role responsibility, adherence to process, architecture design, and cryptographic characteristics of Decentralized Identifiers and Verifiable Credentials produce a safe, efficient, and auditable solution to establishing company identity and authorized trading partner status of trading partners in PI Verifications for saleable returns and, most likely, other DSCSA interactions.

As the solution piloted is based on open standards and the technical documentation created is published openly, the pilot also established that the architecture can be implemented by any company seeking to fulfill one of the piloted roles, thereby ensuring vendor lock-in is mitigated for trading partners.

Lastly, the pilot team has established a roadmap towards implementing the use of Decentralized Identifiers and Verifiable Credentials for DSCSA and is moving to share and execute that roadmap with the whole of the industry.

Pilot Overview

To fulfill the DSCSA requirements, the pilot team sought to test the use of the following components in conjunction with the HDA established Verification Routing Service (VRS):

- W3C specified Decentralized Identifiers (DIDs),
- W3C specified Verifiable Credentials (VCs),
- W3C specified Verifiable Presentations (VPs),
- Verifiable Credential Revocation Registry, and
- Digital Identity Wallets.

These components are described in more detail in the ATP Pilot – Architectural Handbook companion document to this report.

The Challenge

Figure 1 illustrates the difference between a typical "direct" trading partner relationship and an "indirect" trading partner relationship which is required by the statute. The DSCSA requires that trading partners interact only with other trading partners that meet the DSCSA defined Authorized Trading Partner definition. The challenge for trading partners is that, for saleable returns (and other DSCSA use cases), the companies involved represent an indirect trading partner relationship. They have yet to do the proper due diligence on each other to establish each other's identity and DSCSA defined ATP status. The first contact might be a PI Verification event. In order to meet industry defined performance requirements, the piloted architecture was designed to move the process to establish trading partner identity and ATP status off the critical path of day-to-day PI Verifications.

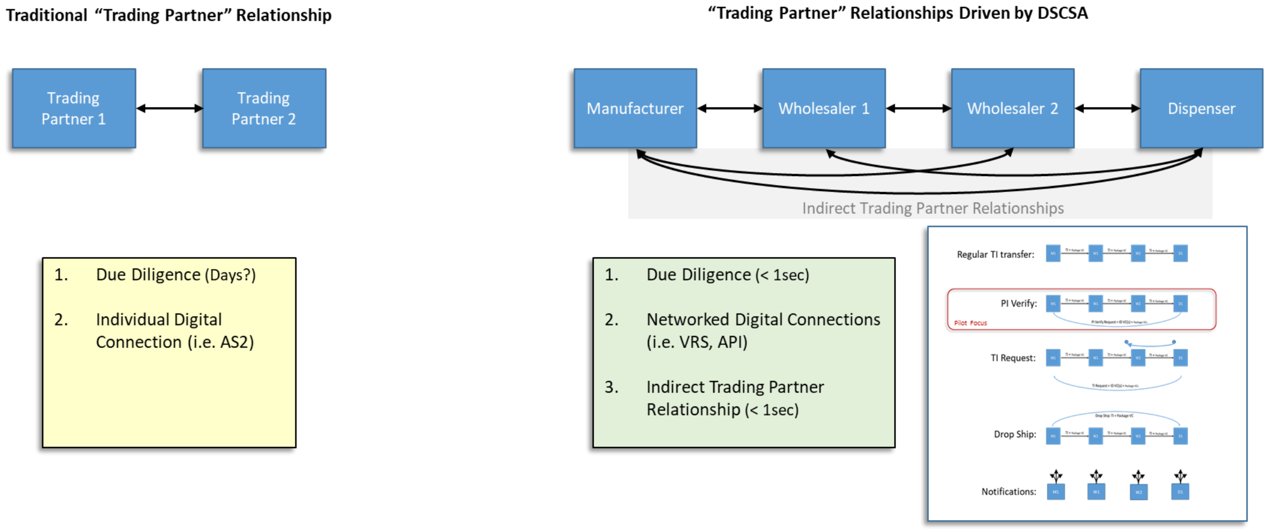

Traditional "Trading Partner" Relationship
Trading Partner 1
Trading Partner 2
1. Due Diligence (Days?)
2. Individual Digital Connection (i.e. AS2)
"Trading Partner" Relationships Driven by DSCSA
Manufacturer
Wholesaler 1
Wholesaler 2
Dispenser
Indirect Trading Partner Relationships
1. Due Diligence (< 1sec)
2. Networked Digital Connections (i.e. VRS, API)
3. Indirect Trading Partner Relationship (< 1sec)
Regular TI transfer:
PI Verify:
Pilot Focus
PI Verify Request + ID VC(s) + Package VCs
TI Request:
TI Request + ID VC(s) + Package VCs
Drop Ship:
Drop Ship: TI + Package VC
Notifications:
M1
W1
W2
D1
TI + Package VC

Figure 1 - DSCSA required indirect Trading Partner Relationships

Establishing Verifiable Credentials for entity identity and ATP status.

Early in the pilot, the team determined that trading partners (see Figure 1) must not only establish that they hold ATP status, but must also establish their identity with each other. Establishing identity and ATP status is key to mitigating nefarious actors from posing as legitimate trading partners and gaining business intelligence from digitally interacting with legitimate trading partners. Figure 2 illustrates the due diligence performed by the credentials issuer in verifying the trading partner's identity and establishing a verified identity credential. That identity credential is checked in the ATP Credential issuing due diligence, along with verifying the trading partner's required licenses. After receiving their Identity and ATP Credentials (in their digital identity wallet), trading partners can use the ATP credential in Product Information Verification interactions to prove their ATP status and verify the ATP status of their trading partner.

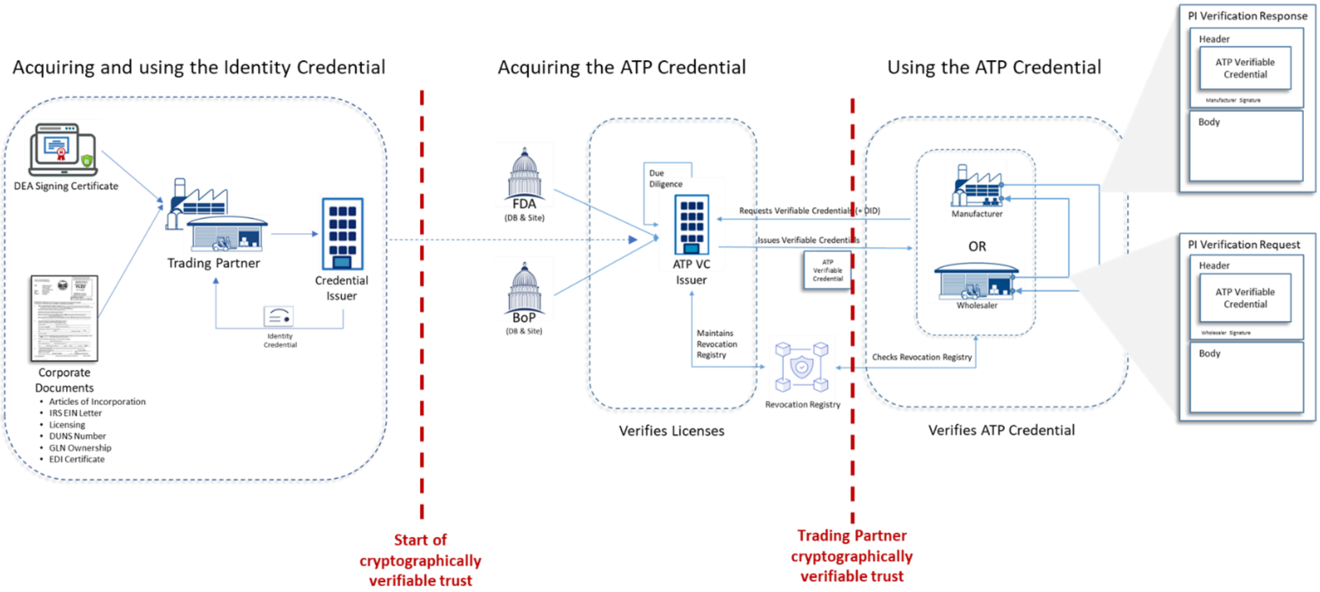


Figure 2 - Overview: The establishment of verifiable trust between adjacent and non-adjacent trading partners

The Credentials

In examining the role of the Verifiable Credential Issuer, the pilot team recognized that the Issuer would need to first perform a rigorous process to establish the identity of a company prior to establishing the ATP status of the company. It was also recognized that there may be Issuers with different capabilities, some choosing to perform the in-depth due diligence necessary to verify a company's identity, and others who might choose to focus on a company's ATP status verification, but would need a simple way to first verify the company's identity.

The Pilot team decided on two separate credentials and processes (due diligence) for Issuing them.

The Identity Verifiable Credential

The Pilot team established that a company can "prove" its identity to an Issuer of the Identity Credential by having an authorized representative:

- Present identifying information about the company; and
- Apply a legal signature to attest that the identifying information is true and accurate.

These two steps to identity proofing can be accomplished either digitally or by submitting paper documents. The digital identity proofing path requires a responsible person[6] in the company to use their digital DEA Signing Certificate in their interaction with the Issuer. The digital DEA signing certificate includes both the company's required identifying information and the signature of the responsible person. If no person in the company has a DEA Signing Certificate, then the identity proofing can take place via the paper documents and "wet" signature path.

[6] DEA Signing Certificates are issued to a responsible person in a corporation. That person must use the signing certificate in the Identity Credential acquisition process to prove their identity and the identity of the company they represent (that the DEA already vetted).

It was felt that the DEA has a rigorous process for establishing a company's identity prior to issuing the digital DEA Signing Certificate, and that nobody but the owner of the certificate would have access to it. Relying on the DEA's due diligence and the security and non-repudiation of the digital signature applied through use of the DEA Signing Certificates allows for a safe and expedited process for issuing the Identity Verifiable Credential.

For those companies without a DEA Signing Certificate, the Pilot team allowed that the Issuer would verify an industry agreed list of documents that the requestor would provide. The Pilot team identified the following documents as examples. Not all companies hold these documents. Documents that provide equivalent Identity establishing value will need to be identified. The Pilot team recognizes that the industry may determine a number of acceptable ways of establishing a company's identity as the use of credentials grows.

- Articles of Incorporation
- IRS Employer ID Number (EIN) letter
- Regulator Issued License
- DUNS number

In addition, the authorized representative would provide a copy of a government issued photo ID, and apply his/her signature by pen to a statement attesting that the documents being submitted for the identity proofing are true and accurate.

An Issuer of the Identity Verifiable Credential must also periodically re-verify the identity of the company. They must also maintain an accessible revocation registry where they establish an entry for credentials that fail re-verification.

The design and schema for the Identity Verifiable Credential can be found in the pilot's Architecture Handbook. The attributes of the Identity Verifiable Credential are:

- Credential ID
- Credential Type
- Issuer
- Credential Issuance Date
- Credential Expiration Date
- Subject Company DID
- Subject Company Name
- Subject Company Address
- Subject Company Contact
- Due Diligence Source
- Due Diligence Signature
- Issuer Signature

The DSCSA ATP Verifiable Credential

In order to issue an ATP Verifiable Credential, an Issuer must first verify the company's Identity Verifiable Credential. The Issuer must then verify the ATP status of the company per the DSCSA, and FDA published guidance. For the purposes of the pilot, the Issuer verified that the trading partner held at least one license for the purposes of doing business as their company type (manufacturer or wholesaler) as defined by the DSCSA.

An Issuer of the ATP Verifiable Credential must also periodically (the pilot team recommends every 24 hours) re-verify the ATP status of the company. They must also maintain an accessible revocation registry where they establish an entry for credentials that fail re-verification.

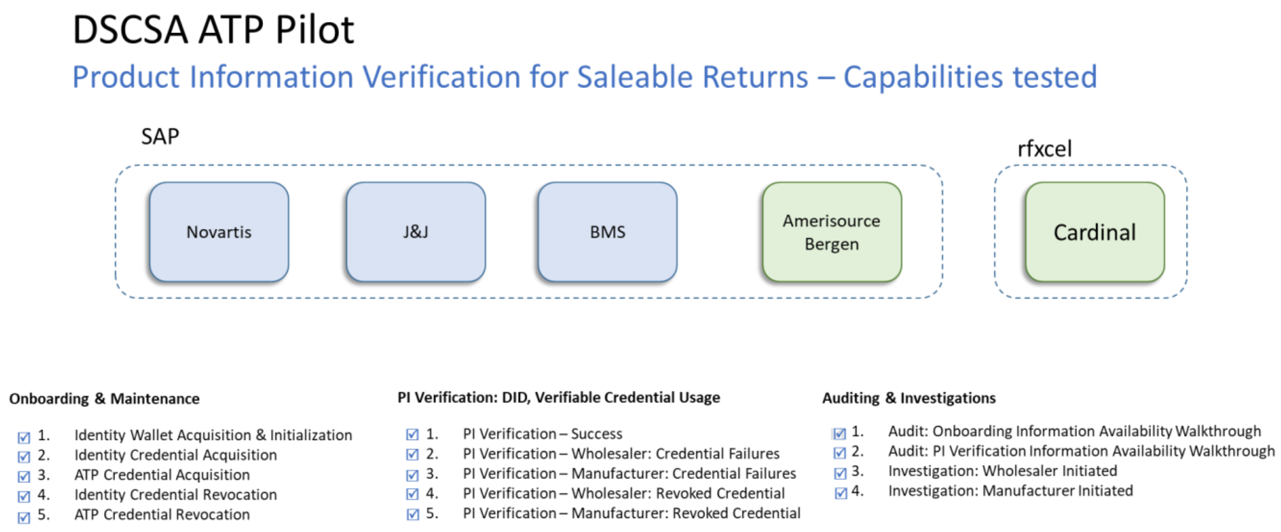
The design and schema for the ATP Verifiable Credential can be found in the pilot's Architecture Handbook. The attributes of the ATP Verifiable Credential are:

- Credential ID
- Credential Type
- Issuer
- Credential Issuance Date
- Credential Expiration Date
- Subject Company DID
- Subject Company Name
- Subject Company Address
- Issuer Signature

Capabilities exercised in the pilot

The pilot participants exercised and proved the architecture was able to support a list of capabilities (see Figure 3) needed to:

1) Acquire a Digital Identity Wallet and establish their Decentralized Identifier which would be used to identify the participant's company throughout the process.
2) Acquire both an Identity and an ATP credential after due diligence from a credential issuer.
3) Interact with other participating trading partners in PI Verifications and provide Identity and ATP credentials in this interaction.
4) Verify the credentials provided by other participants within the process.
5) Assess the ability of the architecture, processes and audit records to support audits and investigations.



DSCSA ATP Pilot

Product Information Verification for Saleable Returns – Capabilities tested

Onboarding & Maintenance

- ☑ 1. Identity Wallet Acquisition & Initialization
- ☑ 2. Identity Credential Acquisition
- ☑ 3. ATP Credential Acquisition
- ☑ 4. Identity Credential Revocation
- ☑ 5. ATP Credential Revocation

PI Verification: DID, Verifiable Credential Usage

- ☑ 1. PI Verification – Success
- ☑ 2. PI Verification – Wholesaler: Credential Failures
- ☑ 3. PI Verification – Manufacturer: Credential Failures
- ☑ 4. PI Verification – Wholesaler: Revoked Credential
- ☑ 5. PI Verification – Manufacturer: Revoked Credential

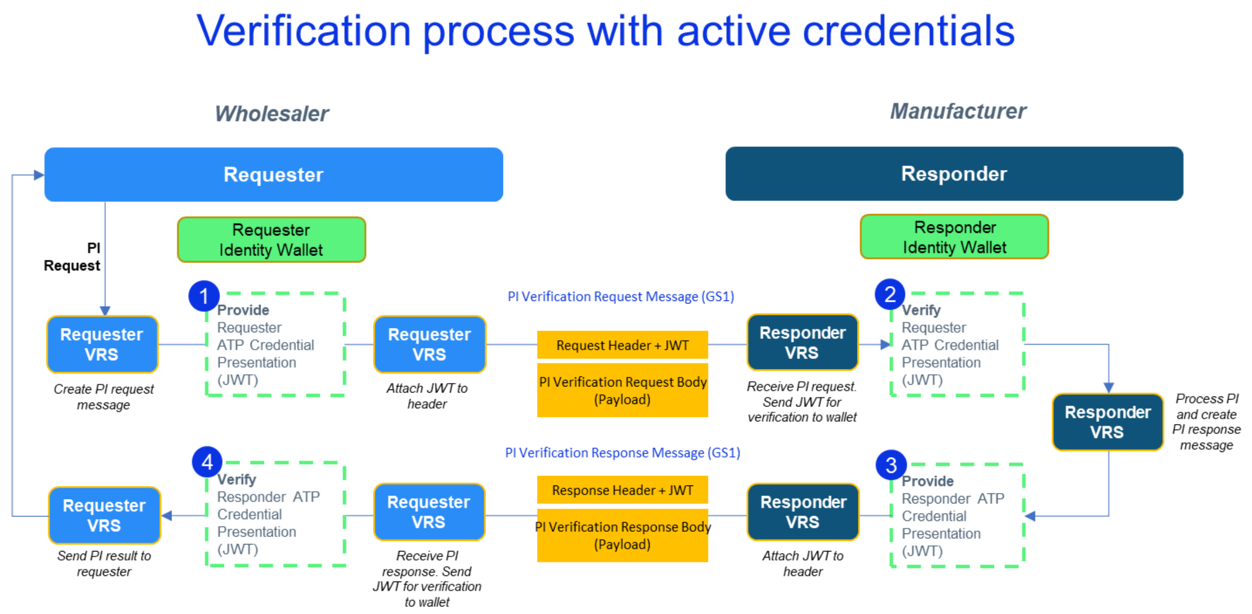
Auditing & Investigations

- ☑ 1. Audit: Onboarding Information Availability Walkthrough
- ☑ 2. Audit: PI Verification Information Availability Walkthrough
- ☑ 3. Investigation: Wholesaler Initiated
- ☑ 4. Investigation: Manufacturer Initiated

Figure 3 - Capabilities tested in the pilot.

Main scenarios exercised, demo cases

The trading partner participants each exercised their industry role (Manufacturer or Wholesaler) in PI Verification exchanges with each other with legitimate credentials (not expired, not revoked as illustrated by Figure 4) and with revoked credentials (illustrated by Figure 5).



Verification process with active credentials

Wholesaler
Manufacturer
Requester
Responder
Requester Identity Wallet
Responder Identity Wallet
PI Request
Requester VRS
Create PI request message
1
Provide Requester ATP Credential Presentation (JWT)
Requester VRS
Attach JWT to header
PI Verification Request Message (GS1)
Request Header + JWT
PI Verification Request Body (Payload)
Responder VRS
Receive PI request. Send JWT for verification to wallet
2
Verify Requester ATP Credential Presentation (JWT)
Responder VRS
Process PI and create PI response message
3
Provide Responder ATP Credential Presentation (JWT)
Responder VRS
Attach JWT to header
PI Verification Response Message (GS1)
Response Header + JWT
PI Verification Response Body (Payload)
Requester VRS
Receive PI response. Send JWT for verification to wallet
4
Verify Responder ATP Credential Presentation (JWT)
Requester VRS
Send PI result to requester

Figure 4 - Verification process with active credentials

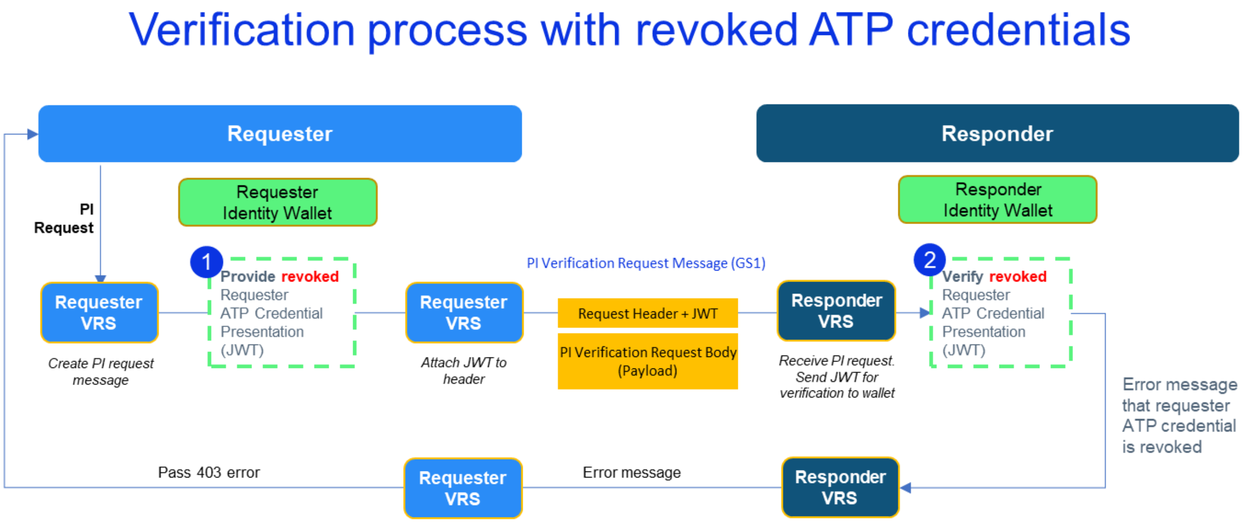

Verification process with revoked ATP credentials
Requester
Responder
PI Request
Requester Identity Wallet
Responder Identity Wallet
1
Provide revoked Requester ATP Credential Presentation (JWT)
PI Verification Request Message (GS1)
2
Verify revoked Requester ATP Credential Presentation (JWT)
Requester VRS
Create PI request message
Requester VRS
Attach JWT to header
Request Header + JWT
PI Verification Request Body (Payload)
Responder VRS
Receive PI request. Send JWT for verification to wallet
Error message that requester ATP credential is revoked
Pass 403 error
Requester VRS
Error message
Responder VRS

Figure 5 - Verification process with revoked credentials

Participants

The pilot team was made up of two levels of participation. “Participants” (Trading Partner, Solution Provider, and Other) were the most active in the pilot, providing guidance, compliance, operations and technical content and actively participated in executing the pilot scenarios. “Trading Partner Observers” attended calls they were able to and provided feedback at key design and execution steps.

Trading Partner Participants:

Company	Type	Key Personnel
AmerisourceBergen	Wholesale Distributor	Jeff Denton, VP, Global Secure Supply Chain Christopher Reed, Sr Dir, Manufacturing Operations Kelly Lacy, Product Owner, Manufacturer Operations Vasudeva Saladi, Mgr, Business Solutions Analysis
Bristol-Myers Squibb	Manufacturer	Brian Lee Diane Redler Priya Viswanathan
Johnson & Johnson	Manufacturer	Bill Janicki Blair Korman Rosemary Hampton
Novartis	Manufacturer	Dan Fritz Dave Mason Sharon Webster Tim Youngberg Amit Deshpande

Trading Partner Observers:

Company	Type	Key Personnel
AbbVie	Manufacturer	Dick Lanier
Atlantic Biologicals	Wholesale Distributor	Karen Moody Daniel Vilavisanis Billy Greer
Endo Pharmaceuticals	Manufacturer	Geoffrey Lackey
Fresenius-Kabi	Manufacturer	Mary Anne Anderson
Gilead	Manufacturer	Anil Dhawan Garrick Heidt Priya Gopal Rathna Arumugam Sumanth Kota
Lilly	Manufacturer	Senthil Rajaratnam
Merck	Manufacturer	Dave Rendanauer Suzanne Clark
Par Pharmaceuticals	Manufacturer	Aladin Alkhawam
Kaiser Foundation Hospitals	Dispenser	Stephan Baur

Solution Provider Participants:

Company	Type	Key Personnel
Legisym	Credential Issuer	David Kessler Penny Hendrix Britany Payson Steve Carter
rfxcel	VRS Provider	Herb Wong Brian Files Atul Mohidekar Packiaraj
SAP	VRS Provider	Oliver Nuernberg Abdul Musavir Neha Kumari
Spherity	Digital Wallet Provider	Carsten Stoecker Georg Juergens Michael Ruether Adam Martin

Other Participants:

Company	Type	Key Personnel
Center for Supply Chain Studies	Facilitator	Bob Celeste
GS1	Standards Organization	Gena Morgan Neil Aeschliman
HDA	Industry Association	Justine Freisleben Tish Pahl, (OFW Law) Rachel Newman

Goals & Objectives

The objectives of the ATP pilot are to provide evidence on:

1. The feasibility of meeting DSCSA ***compliance goals*** with a DID, VC credential, and Identity Wallet approach in a minimally invasive way,
2. ***Operational goals*** such as response times, scalability, and ease of integration with existing business processes, and
3. ATP credential ***verifiability in a digital chain of trust.***

Compliance goals:

Wholesaler:

- Know who responds to a verification request.
- Determine whether responders meet the ATP threshold.
- Prevent bad actors from interacting.
- Credential:
    - Acceptable by regulator
    - Meets due diligence goals
- Credential revocation checks meets the frequency occurrence goal (see considerations).

Manufacturer:

- Know who is requesting verification.
- Determine whether requesters meet the ATP threshold.
- Prevent bad actors from interacting.
- Credential:
    - Acceptable by regulator
    - Meets due diligence goals
- Credential revocation checks meets the frequency occurrence goal (see considerations).

Issuer:

- Know who is requesting credentials.
- Determine whether requesters meet the ATP threshold.
- Revocation checks meet the frequency occurrence goal (see considerations).

Operational goals:

- < 1 sec end-to-end round-trip time for a verification request.
- Benchmark against VC-free scenario.
- Analyze different VC data structures and types (e.g., Identity Verification VC, ATP VC, VCs on corporate level or on facility level).
- Provide performance metrics for comparison.
- Comparison between alternative business logic (batch vs real time, 1st contact vs subsequent).

Digital Chain of Trust goals:

- Pilot establishes a digital "chain of trust" based on agreed due diligence standards and cryptographically verifiable identifiers and credentials that validate compliance with them.

- This digital “chain of trust” is the key to the value of the system and interacting with it meaningfully becomes the gateway to operating in the supply chain.
- The critical points are where trust proof crosses over from the physical world to the digital world (the due diligence). These trust proofs shall be analyzed in this project.
- Demonstrate the use of W3C specified Decentralized Identifiers, Verifiable Credentials and Presentations to prove DSCSA ATP status of both trading partners involved in the verification of Product Information.
- Identify workable credentials.
- Establish a workable credential issuing process and due diligence standards.
- Prove the auditability of the eco-system to investigate ATP interactions.
- Demonstrate real-time PI Verifications and failures due to license or identity issues.
- Remain within the industry established performance requirement for PI Verification (< 1 sec).
- Consider other DSCSA use cases.
- Identify industry governance requirements.
- Identify standardization opportunities.

ATP Pilot Team Statement

The statement reflects the participants' understanding of the DSCSA trading partner identity issue, what they seek to accomplish through the pilot and their hypothesis of the solution.

ATP Pilot Statement:

The Pilot team recognizes that:

- The DSCSA requires manufacturers, repackagers, wholesalers and dispensers to only trade with companies that meet the DSCSA defined “Trading Partner” and “Authorized” definitions.
- Compliance with the DSCSA will require supply chain companies to digitally interact with other supply chain companies where the company identity and the DSCSA defined “Trading Partner” and “Authorized” status will be unknown at the time of interaction.
- In order to complete the interaction, it is essential for companies at both ends of a DSCSA digital interaction to know the identity of the other company and if the other company meets the DSCSA defined “Trading Partner” and “Authorized” definition.

The pilot team sought to pilot the use of W3C (World Wide Web Consortium) standard decentralized Identifiers (DIDs) and verifiable credentials (VCs) in conjunction with the GS1 Lightweight Messaging Standard to:

- Know the identity of PI Verification requestors and responders.
- Verify that the requestor or responder meets the DSCSA definition of “Trading Partner” and “Authorized”.

The Pilot team believes, given no unforeseen circumstances, that:

- the proposed verifiable credentials content, use of decentralized identifiers and processes for issuing, maintaining, and revoking verifiable credentials will meet the identity, DSCSA "Trading Partner" and DSCSA "Authorized" definition for their companies.

Piloted Roles

Pilot team members enacted the responsibilities defined by their role.

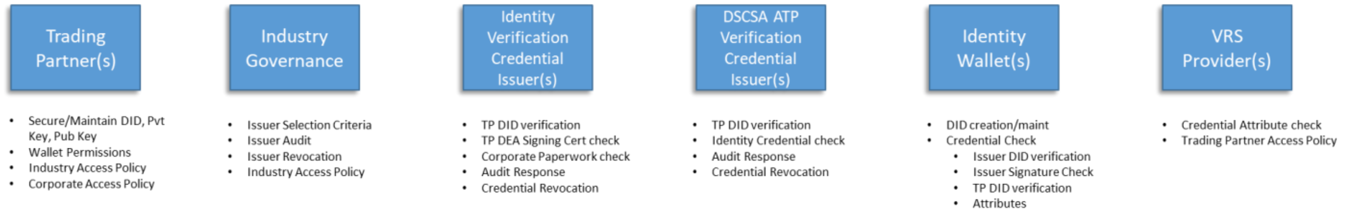


Figure 6 - Piloted Roles and Major Responsibilities

Key Components of the Piloted Solution

The Proof of Concept that Novartis, SAP, and Spherity completed prior to the pilot demonstrated the architecture and technologies that the pilot would expand upon. However, design sessions and discussions with compliance and business operations team members quickly highlighted the importance non-technical solution components would play. Figure 7 illustrates the team's main finding, that these technical and non-technical components must work together to form the whole solution that is needed from compliance, business operations, and technical perspectives.

Component	Contribution
Decentralized Identifiers (DIDs)	● Self-Issued, self-managed by the Trading Partner and Issuer ● Verified via associated published Public Keys ● Associated Private Key used to sign Verifiable Presentations
Verifiable Credentials	● Issued by trusted Issuers ● Tamper evident ● Proof of who the Trading Partner is and that they have ATP Status ● Verifiable without contacting Issuer ● Verifiable Issuer DID and Signature Verifiable Trading Partner DID part of the Issuer verified data

Component	Contribution
Verifiable Presentations	● Includes the ATP Verifiable Credential and hash of the PI Verification request or response ● Provides proof that the transaction was initiated by the Trading Partner ○ Signed by the Trading Partner ○ Signature verified via associated Public / Private keys
Architecture	● PI Verification Requests / Responses use GS1 Standard Lightweight Messaging Standard messages with the Open ATP stack ● Open ATP stack includes: Trading Partner's Verifiable Credential wrapped in a Verifiable Presentation that is signed by Trading Partner, includes a hash of the PI Verification Request or Response ● Exception handling support
Compartmentalized Access	● Credential Issuers and Wallet Providers – no access to business transactions ● Only Trading Partner has control and access to Private Key(s) ● Trading Partner, Issuer – control their own DID and key management
Due Diligence	● Credential Issuers and Wallet Providers – no access to business transactions ● Only Trading Partner has control and access to Private Key(s) ● Trading Partner, Issuer – control their own DID and key management
Roles and Responsibilities	● All Parties create and archive audit records which include the transaction UUID ● Issuer verifies Trading Partner's DEA Signing Certificate or corporate documents to establish Trading Partner Identity ● Issuer verifies Trading Partner's role license to establish ATP ● Issuer

Interoperability Strategy

It was the intent of the pilot participants that an open architecture be piloted, and not a single vendor's solution. It was also the intent of the pilot team that the architecture components should be made available to Standards Bodies for standardization and industry acceptance.

The pilot demonstrates an open architecture that can be implemented by any entity seeking to fill the role of VRS Provider, Credential Issuer, or Digital Wallet Provider. In that respect, the open architecture mitigates against vendor lock-in, and should be standardized and agreed to by the industry.

The team believes that this architecture supports the needs of all stakeholders. However, in the event that multiple ATP schemes are desired by the Trading Partner community, the community should consider the following interoperability points:

- **Performance:** Multiple architectures to determine Identity and ATP status will have a performance toll on the whole system.
- **Cost:** Multiple architectures could be costly as VRS Solutions would be required to code for each architecture and develop verifiable cross-walks between systems.
- **Equivalency in due diligence:** any Identity and ATP assessing architecture will necessarily require a certain due diligence to be performed to verify a trading partner's documentation, be it digital or paper. Unless the due diligence is required to be the same exact check and verifications, the mechanism of proving ATP Status may be acceptable in both systems but be different.
- **Equivalency in architecture:** Figure 7 illustrates the key components of the piloted solution. Each component must be matched in some form by other architectures, otherwise the trustworthiness of the whole system could suffer.
- **Audits and Investigations:** the audit record definitions and SOPs between two different architectures must be examined to determine equivalency and how records will be transited between the architectures.
- **System Validation:** Multiple architectures add complexity for system validators.

Compliance and Validation Strategy

The pilot team was able to present an overview of the pilot during the FDA's Pilot Program update workshop held December 8 and 9, 2021. The team will present this Pilot Report to the FDA and is scheduling a deep dive on the pilot with FDA staff. The team seeks to present the architecture as contributing to the compliance of the ATP validation requirements of the DSCSA.

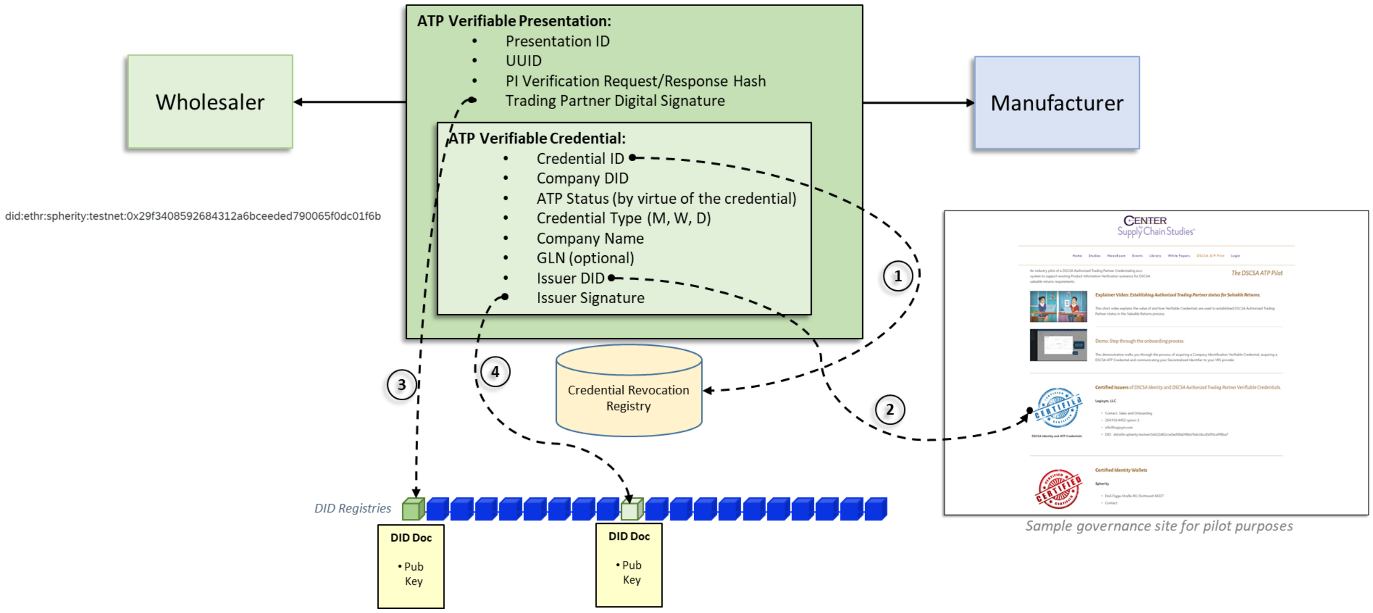
From the perspective of determining the DSCSA defined Authorized Trading Partner status of entities who are PI Verification requestors (wholesalers) and responders (manufacturers), the piloted solution provided:

- a tamper evident credential and presentation to determine ATP Status
- cryptographic means to determine the trading partner and Issuer signatures
- based initial identity determination in the secure DEA process of issuing DEA Signing Certificates
- a means for small and medium companies to participate via a corporate document verification process

- a means (revocation registry and Issuer responsibilities) to determine if corporate identity or ATP status had changed
- audit records and identifiers (UUID) to correlate information exchanged and processes executed between piloted systems in order to support audits and investigations

Technologies Addressed

The pilot explored the use of W3C standard Decentralized Identifiers and Verifiable Credentials. Figure 8 shows key components of Decentralized Identifiers, Verifiable Credentials, and their related Revocation Registry.


ATP Verifiable Presentation:
Presentation ID
UUID
PI Verification Request/Response Hash
Trading Partner Digital Signature
ATP Verifiable Credential:
Credential ID
Company DID
ATP Status (by virtue of the credential)
Credential Type (M, W, D)
Company Name
GLN (optional)
Issuer DID
Issuer Signature
Wholesaler
Manufacturer
did:ethr:spherity:testnet:0x29f3408592684312a6bceeded790065f0dc01f6b
1
2
3
4
Credential Revocation Registry
DID Registries
DID Doc
• Pub Key
DID Doc
• Pub Key
CENTER for Supply Chain Studies
Home
Studies
NewsRoom
Events
Library
White Papers
DSCSA ATP Pilot
Login
CERTIFIED
CERTIFIED

The DSCSA ATP Pilot

An industry pilot of a DSCSA Authorized Trading Partner Credentialing eco-system to support existing Product Information Verification scenarios for DSCSA saleable returns requirements.

Explainer Video: *Establishing Authorized Trading Partner status for Saleable Returns.*

This short video explains the value of and how Verifiable Credentials are used to established DSCSA Authorized Trading Partner status in the Saleable Returns process.

Demo: Step through the onboarding process.

This demonstration walks you through the process of acquiring a Company Identification Verifiable Credential, acquiring a DSCSA ATP Credential and communicating your Decentralized Identifier to your VRS provider.

DSCSA Identity and ATP Credentials

Certified Issuers of *DSCSA Identity* and *DSCSA Authorized Trading Partner* Verifiable Credentials.

Legisym, LLC

- Contact: Sales and Onboarding
- 254.933.4452 option 3
- info@Legisym.com
- DID: did:ethr:spherity:testnet:0xb22d82cca0ed58a098b67bdc6bcd0d10ca9f8ba7

Certified Identity Wallets

Spherity

- Emil-Figge-Straße 80, Dortmund 44227
- Contact:

Sample governance site for pilot purposes

Figure 8 - Verifying the Verifiable Credentials

Once a Verifiable Credential and Verifiable Presentation are received by a VRS provider (or directly by a Trading Partner in some cases), the information they contain can be cryptographically verified. In addition, attributes and metadata in the Verifiable Credential and Verifiable Presentation can be checked against other data the Trading Partner already has possession of.

- The Universally Unique ID (UUID) in the verifiable presentation must match the UUID in the PI Verification Request or Response.
- The PI Verification Request or Response Hash value must match a Hash value calculated from the PI Verification Request or Response itself (without the XATP Header containing the Verifiable Presentation and ATP Verifiable Credential).
- The Trading Partner Digital Signature must match a signature created using the Private Key associated with the Company DID found in the ATP Credential. This shows that the Trading Partner identified by the Company DID, did execute the PI Verification Request or Response.

  a. The check is accomplished with the Public Key associated with the Company DID, which can be found using the Company DID to retrieve the DID Document as specified by W3C standards.

- The ATP Verifiable Credential must not be revoked. This can be checked by accessing the Issuer's Revocation Registry and ensuring the Credential ID is not listed as "revoked".
- The ATP status of the Trading Partner is established by the presence of the ATP Verifiable Credential.
- The Credential Type must match the action taken by the Trading Partner.
  a. Credential Type must be "W" if this is a PI Verification Request for a Saleable Return.
  b. Credential Type must be "W" or "D" if this is a PI Verification Request for an Investigation (future requirement).
  c. Credential Type must be "M" if this is a PI Verification Response.
- The Company Name is the Trading Partner's corporate entity name that the ATP Verifiable Credential Issuer verified prior to issuing the credential.
- The GLN is an optional attribute[7] and will be used to explore usage of a future GLN credential.
- The Issuer DID must be a "well known DID" by being published by a trusted source that has certified the Issuer and verified the DID.
- The Issuer Digital Signature must match a signature created using the Private Key associated with the Issuer DID found in the ATP Credential. This shows that the Entity identified by the Issuer DID, did complete the required due diligence for the Identity Credential and the ATP Credential issued to the Entity identified by the Company DID.
  a. The check is accomplished with the Public Key associated with the Issuer DID, which can be found using the Issuer DID to retrieve the DID Document as specified by W3C standards.

ROI Opportunities

Throughout the pilot, the team discussed other opportunities to use the core piloted components of Decentralized Identifiers, Verifiable Credentials and the architecture and support services needed to manage them. The team sees potential in using this architecture for other DSCSA related use cases such as:

- Product Information Verification for Investigations
- Transaction Information (TI) Request / Response
- Drop Shipments
- Transaction Information Transfer
- Recalls

The team is also aware of, and in some cases, actively pursuing or know others that are pursuing the use of this technology for new business interactions and to bolster existing business interactions.

[7] Additional attributes may be added at a future time to facilitate investigations.

Considerations

Cost

Assumptions

1. Each trading partner needs an identity wallet, credential issuer and a VRS provider.
2. The VRS provider will need to make changes in the existing implementation to accommodate the ATP Credentialing Service.
3. Large organizations will need more formal audit, investigation and system validation support.
4. Small organizations will need simpler solutions.
5. Invested costs will decrease as use increases across the industry and as credentials are used in new use cases.

Cost drivers

Cost drivers for trading partners using the piloted implementation. These cost drivers influence the price of ATP Credentialing depending on the internal setup, the configurations and customizations. As these cost drivers differ, trading partners have different cost structures:

- Audits and system validation
  - Large corporations may...
    - perform formal audits and request reporting from selected vendors
    - require documentation for GxP process and system validations
    - have multi-purpose requirements
  - Small companies may…
    - need simpler or standardize audits and reporting from selected vendors
    - ...
- Review of 3d party vendors
  - Large corporations may ...
    - need Software as a Service assessments
    - make security investigations
    - require vendor accreditations
    - require specific certifications
    - require multiple reviews of contractual documents
  - Small companies may …
    - need standardized service descriptions
    - organize each other in associations to bundle and standardize the vendor onboarding effort
- Capabilities
  - Large corporations may ...
    - require customized features
    - extended analysis and alerts
    - customized Identity Access Management (e.g. Active Directory Integration)
    - have security requirements
    - have individual deployment requirements (local vs. SaaS)
    - have individual data storage requirements

    - Small companies may …
        - use a standardize service offering

- Make or buy
    - Large corporations may …
        - buy a license from a service provider
        - enter a Software as a Service agreement
        - build an own ATP Credentialing service
    - Small companies may
        - enter a Software as a Service agreement

Service Models

The trading partner might have options to use the ATP Credentialing Service.

- Trading partner directly contracts ATP Credentialing Service provider
    - Trading partner needs to enter new contract(s) with service provider(s)
- Trading partner uses an ATP Credentialing feature from his VRS
    - Extending the existing contract with VRS (if VRS has integrated ATP Credentialing Service capabilities)

Considering the cost drivers and the service models, a productive system to use ATP Credentialing is projected (for large corporations and small businesses) to be a reasonable investment.

Adoption and Implementation

Upon the successful conclusion of the pilot, the team recommends moving to a pre-production (production ready and optional) environment for the piloted architecture.

Based on the pilot work, the involved trading partners, service providers and facilitators agreed on establishing a “Open Credentialing Initiative”, that

- is the “brand” of the piloted implementation
- includes a set of authentication services used to meet the needs of ATP
- is an open and standards based framework that can be implemented by various organizations
- governs the next phase of the pilot, with the objective to bring it to production.

Additional DSCSA Use Cases

PI Verification for Investigations

In 2023, Wholesalers and Dispensers must be able to verify the Product Information of a drug package in the instance of an investigation. The architecture piloted can be used for this use case also. However, the “reason” attribute in the PI Verification message (context=dscsaSaleableReturn) must be able to carry additional values beyond “saleable return”.

TI Request (Trace)

In 2023, trading partners must have *“The systems and processes necessary to promptly facilitate gathering the information necessary to produce the transaction information for each transaction* *going back to the manufacturer, as applicable".*[8] The pilot team has recommended that the Identity and ATP credentials be explored as a way to establish a safe means for trading partners to enhance TI Requests and TI Responses.

Drop Shipments

In the case of a drop shipment, the Manufacturer and the Dispenser may also need to verify each other's identity and ATP Status. The piloted architecture could be used based on an industry agreed Drop Shipment process and associated messages.

Governance Considerations

As the pilot progressed, a number of decisions needed to be made in order to move forward. The pilot team recognized that the industry must consider these same issues and come to a consensus under a governance construct. The list below constitutes the governance topics that the team encountered, and the decision reached for the pilot.

Credential Revocation Check Frequency

Identity Verifiable Credential

Mergers, acquisitions and other identity-changing events occur within the industry. It is recommended that Issuers adopt a process to re-verify the identity proofs that were used to establish the Identity Credential annually and revoke any Identity Credential that cannot be verified. Ultimately, this frequency will be established via industry consensus.

ATP Verifiable Credential

Issuers: State Board of Pharmacy licenses for wholesalers (and dispensers) are publicly updated based on the frequency set by each State or triggered by inspection outcomes. For example, a State might revoke a license and publish the revocation on their regular schedule (weekly, monthly, on demand). This is the same situation with FDA Establishment Identifiers (FEI) for manufacturers. It is recommended that Issuers verify State Board of Pharmacy issued licenses and FEIs every 24 hours to ensure a minimal amount of time for ATP status changes to be available to trading partners. Issuers must revoke any ATP Credential where underlying licenses or FEIs cannot be verified.

Trading Partners (manufacturers and wholesalers): Based on the above considerations and potential timing differences between the timing of a regulator updating their public information and the Issuer's re-verification process, it is possible for ATP status changes to only be accurate greater than 24 hours (this is still a large improvement over current availability). It is recommended that trading partners ensure their Identity Wallets verify every 24 hours that credentials are not revoked. In practical terms, this means they should refresh local copies of revocation information every 24 hours.

[8] This is a requirement of Sec 203 - Enhanced Drug Distribution Security section of the Drug Supply Chain Security Act currently effective November 27, 2023.

Government Agencies

To address the issue of variations of when the regulator's information is publicly accessible via the regulator's mechanism for disseminating license information, inspections and audits should take into consideration the cadences of when license update information is available, and systems are able to act on that information.

Today, regulators provide license and registration information via web pages, spreadsheets etc. Regulators should consider providing licenses registrations in the form of Verifiable Credentials, essentially creating verifiable[9] licenses and registrations. This could serve as a system-wide strengthening mechanism to ensure license and registrations could only be used by entities they were issued to. Also, industry stakeholders could benefit by the use of these now verifiable licenses and registrations in other use cases requiring assurance of identity and authorization.

Data Retention

In order for the system to be useful in supporting investigations, the team recommends that data retention rules be in alignment with the DSCSA rules for archiving TI; to maintain the information six years after transacting the product or six years after an investigation. Given the order of transactions in the supply chain, manufacturers will necessarily reach the six-year mark before subsequent wholesale distributors or dispensers. The team also recommends the industry determine a fair retention time so as not to leave trading partners with no recourse for investigations.

Standardization

In the course of the pilot, the pilot team discovered a number of areas that would benefit from standardization. These areas were discussed with GS1, and the plan is to further investigate standardization and timing to develop or enhance the necessary standards or guidelines.

Applying the GS1 Lightweight Messaging Standard for DSCSA Verification of Returned Product Identifiers (Implementation Guide)

The pilot utilized the GS1 Lightweight Messaging Standard to also carry the ATP Credential in the header of PI Verifications and PI Responses. The Team recommends that GS1 US provide for this option in the implementation guide.

GS1 Lightweight Messaging Standard

The ATP Credential and verifiable presentation were placed in a distinct header within the header of the PI Verification Request and the PI Verification Response. The pilot team believes there is no change needed to the Standard in order to use it in this way. The team has provided GS1 US a copy of the ATP Credentialing Pilot Security Analysis that explores the main security vulnerabilities and how the use of verifiable credentials issued against decentralized identifiers might mitigate those vulnerabilities.

Credential Schemas

[9] At the time of presentation or use of a verifiable credential, the recipient can cryptographically determine if the presenting system is the subject of the credential and whether the credential has not expired or been revoked.

As the intent of the pilot was to create an open solution, the pilot team is working with GS1 US to standardize the schemas and the credential attributes.

GS1 Web Vocabulary

GS1 maintains a web vocabulary which is designed to extend the work done by schema.org and makes use of similar concepts (Product, Offer, Organization), extending them with many more details. As the definitions defined in the vocabulary are already used in attributes of GS1 B2B messages and EPCIS events, the pilot team is working with GS1 to normalize the definitions of the piloted vocabulary.

GLN Credential

The industry has moved to using the GS1 EPCIS Standard[10] to exchange serialized Transaction Information (TI) and Transaction Statement (TS) information. The EPCIS Standard makes use of the GS1 GLN (Global Location Number) to identify trading partners in TI exchanges. GS1 US is exploring issuing GLN verifiable credentials. To make room for this exploration, the pilot Identity credential includes the GLN as an optional attribute. This allows for future discussions on the use of a GLN verifiable credential in the Issuer due diligence process for establishing the Identity Credential.

Root of Trust Discussion

A Root of Trust (RoT) is a source that can always be trusted within a cryptographic system. Currently, the pilot team has established the Identity Credential as the pilot's Root of Trust, and issuance of ATP Credentials is dependent on the verifiable Identity Credential. In the pilot, the trading partners established the due diligence expected of the Credential Issuer. The Credential Issuer exercised this due diligence prior to issuing credentials. The due diligence contained automated and manual processes.

ATP Pilot - Root of Trust establishment and credential issuance due diligence rules:

For the purposes of the ATP Pilot, the Identity Credential is the Root of Trust and the ATP Credential is issued based on the presentation of the Identity Credential to an Issuer.

As such, we are able to establish a cryptographically verifiable chain of trust from any point in the pilot scope leading back to this one Root of Trust.

In order to establish that the Identity Credential is the Root of Trust for our pilot eco-system, the pilot team needed to agree that the Issuer's Due Diligence process is sufficient and auditable.

For the purposes of the pilot, the pilot team agreed that the following documentation is required as input to the Issuer's due diligence process for creating an Identity Credential.

[10] GS1 US Implementation Guideline for Applying GS1 Standards for DSCSA and Traceability, *https://www.gs1us.org/industries/healthcare/standards-in-use/pharmaceutical/implementation-guideline*

Identity Credential

1. Use of DEA Signing Certificate to prove identity and establish the provided DID as the corporate DID.

or

2. The following corporate documents would be presented:
    a. Articles of Incorporation,
    b. IRS Employer Identification Number Assignment letter,
    c. DUNS number,
    d. For entity responsible Party:
        i. Name,
        ii. Address,
        iii. Corporate email address,
        iv. Photo ID (copy),
        v. DUNS number,
        vi. Notarized Identity Credential Request letter (signed by Corporate Responsible Party)

ATP Credential

The DSCSA (and FDA Guidance) define "Authorized" as an entity that has the proper license, application or registration for their role. State Boards of Pharmacy issue licenses for each location of a wholesaler or dispenser, there is no "corporate" license as a corporation can operate within many States.

The challenge is for Saleable Returns PI Verification. Until November 27, 2023, the supply chain is not required to exchange serialized information on shipments, and a wholesaler is not required to pass TI/TS to move products to any location under its control.

So, for PI Verification, supporting Saleable Returns, the location of the product is unimportant and possibly unknowable until 2023, when serialized transfer information is shared.

For the purposes of the PoC and the Pilot, the ATP Credential represents that:

1) The Issuer has performed the following due diligence:
    a) Verified the Identity Credential that the ATP credential requestor presents.
    b) Received an ATP Credential request and verified the following information:
        i) Company Legal Name
        ii) Company Address
        iii) Responsible Person Name
        iv) Responsible Person Phone Number
        v) Responsible Person email address
        vi) Company DID

c) Validated a corporate email address of the Responsible Person.
d) Verified that the credentials requestor holds at least one (1) valid:
   i) State Board of Pharmacy license (for wholesalers or dispensers) or
   ii) FDA Establishment Identification (FEI) number (for manufacturers)

2) The issuer will perform a periodic verification (see 1d above) every 24 hours for the duration of the credential (credential effective date through credential expiration date).
3) The Issuer will revoke the credential via an entry in the revocation registry should the periodic verification fail.

Audit Requirements

A separate document was created detailing the audit requirements for the integration of Identity Wallets, Identity Credentials and ATP Credentials. A link to that document can be found in the Purpose of this Document section at the beginning of this report.

Lessons Learned / Conclusions

Comments from pilot team members:

DSCSA Compliance

"A cross functional team realized there was a compliance issue with digital systems and assuring an Authorized trading partner (ATP.) is using the digital system. The credentialing process is the first proven industry digital process that addresses ATP compliance gap of knowing if the company is an Authorized Trading partner per DSCSA requirements using the system This is a foundation for 2023."

… Dave Mason, Novartis Supply Chain Compliance and Serialization

Inspection Readiness

"Assurance that the FDA's Data Integrity compliance indicators and the DEA Standards for Electronic Transmissions (Authentication, Nonrepudiation and Message Integrity) are incorporated in this solution."

… Sharon Webster, Novartis Pharmaceutical, AD Market Product Quality

Technical Requirements

"As a VRS solution provider, all we had to do was a simple API-call to the wallet to retrieve or verify credentials and some small changes to handle the response from the wallet. All in all, this technology allows us to implement the ATP check in the existing – and established – processes without disruption."

… Oliver Nuernberg, Chief Product Owner, SAP Life Sciences

"Including the ATP credential in the message to secure the network is a good idea. The upfront due diligence by the issuer in creating the credentials would be important to the archive/audit trail that was piloted. This solution would need broad adoption."

… Rosemary Hampton, J&J Information Technology

"The ATP pilot is the most comprehensive effort to address the upcoming Authorized Trading Partner requirement for DSCSA. rfxcel was impressed to see how seamlessly it integrated with our solution. All participants work well together and rfxcel is excited to see this adopted by other solution providers and the industry."

… Herb Wong, VP Marketing & Strategic Initiatives, rfxcel

Implementation

"The pilot effort was very organized. Once we received the specs, it took us one week to implement the solution and begin testing."

… Herb Wong, VP Marketing & Strategic Initiatives, rfxcel

Interoperability

"The piloted solution requires no change in GS1 Lightweight Messaging Standard currently used for PI Verification. The team intends to submit Application Programmer Interface (API) and credential schema designs to GS1 US for Standardization or Guidance inclusion."

… Bob Celeste, Founder, Center for Supply Chain Studies

Adoption

"Using ATP credentials for PI Verifications or Tracing is just the tip of the iceberg. The provided enterprise identity wallets and credentials will change the way trading partners digitally interact with each other. DID and VC solutions have the potential to be used and adopted as well in other supply chain use cases."

… Georg Juergens, Manager, Spherity

Next Steps – ATP Credential Roadmap

With the successful completion of the pilot, the team recommends a roadmap toward production use of the piloted architecture, processes, and procedures. In the near term, the team recommends a phased approach to achieve a pre-production environment for trading partners and VRS providers to implement toward production usage in 2023.

Socialization, Education and Acceptance

Socialization and Education have been ongoing. The pilot team holds monthly update calls with the industry at large and with the HDA VRS community of trading partners and solution providers. The team has also provided presentations to the FDA as part of their DSCSA Pilot Program meeting in December of 2020 and for the Partnership for DSCSA Governance (PDG). The team recommends that this outreach effort continue through 2021. The team has reached out to VRS providers and Dispensers to explore the pilot architecture.

PI Verification (VRS provider connect via VRS routing)

This phase will include changes to a trading partner's current VRS system to allow for VRS routing of ATP Credential enhanced PI Requests.

In this phase, credentialing needs to be implemented with the following boundary conditions:

- The implementation of credentialing must not impact the existing verification process.
- The addition or verification of DID/VCs is optional.
- The implementation allows a gradual change to the way VC/DID are used and verified.

As a requester who may already use credentials does not know which entity acts as a responder and whether that entity may or may not use credentials, the optional use and check of credentials is important. A way to achieve this is to allow requesters and responders to start adding and checking credentials at their own pace. For example, the following options may be provided:

ATP Credential usage maturity

- Including Credentials
    - Credential is NOT added when sending request or response
    - Credential is added in responses only when the request contains a Credential
    - Credential is always added when sending request or response
- Checking Credentials
    - no Credential check is executed
    - Credential Check is executed, but with no impact. A request or response is accepted regardless of whether the Credential can be verified or not.
    - Credential Check is executed. If the Credential cannot be verified an error is triggered and request or response is NOT accepted.

PI Verification for investigations (Dispensers)

The team believes the piloted architecture and credentials can also be used for PI Verifications to support Suspect and Illegitimate product investigations. This phase will include manufacturers, wholesalers, and dispensers and may run in parallel with Phase 1 or 2.

TI Request (Trace)

Usage of the Identity and ATP credential for TI Requests and Responses will be explored and architected.

Other DSCSA use cases.

The DSCSA includes other use cases that might benefit from the use of the piloted and other credentials. Those use cases are:

(i) TI/TS Transfer
(ii) Drop Shipments
(iii) Notifications

Industry Adoption Readiness - It is anticipated that the use of the ATP Credential will remain optional as the industry implements over the next few years. The ATP Credential usage maturity section above depicts the landscape Trading Partners and VRS Providers should expect to encounter as adoption moves forward.

Appendix

Acronyms and Terms

Acronyms and terms used throughout this document are defined here.

Authorized Trading Partner (ATP)[11]

DSCSA restricts access to the distribution system for prescription drug products by requiring trading partners of manufacturers, wholesale distributors, dispensers, and repackagers to meet the applicable requirements for being authorized trading partners.[12] DSCSA includes definitions for *authorized*[13] and *trading partner*[14] with respect to each entity in the drug supply chain as follows:

- To be considered an authorized trading partner, a *manufacturer* or *repackager* must have a valid registration in accordance with section 510 of the FD&C Act and accept or transfer direct ownership of a product from or to a manufacturer, repackager, wholesale distributor, or dispenser.

- To be considered an authorized trading partner, a *wholesale distributor* must have a valid license under State law or section 583 of the FD&C Act, in accordance with section 582(a)(6) of the FD&C Act , comply with the licensure reporting requirements in section 503(e) of the FD&C Act, as amended by DSCSA, and accept or transfer direct ownership of a product from or to a manufacturer, repackager, wholesale distributor, or dispenser.

- Similarly, to be considered an authorized trading partner, a *3PL* must have a valid license under State law or section 584(a)(1) of the FD&C Act, in accordance with section 584(b) of the FD&C Act (21 U.S.C. 360eee-3) and accept or transfer direct possession of a product from or to a manufacturer, repackager, wholesale distributor, or dispenser.

- A *dispenser* must have a valid license under State law and accept or transfer direct ownership of a product from or to a manufacturer, repackager, wholesale distributor, or dispenser.

Claim

An assertion made about a subject.

Decentralized Identifier (DID)

A portable URL-based identifier, also known as a ***DID***, associated with an entity. These identifiers are most often used in a verifiable credential and are associated with subjects

[11] See "Identifying Trading Partners Under the Drug Supply Chain Security Act", FDA Draft Guidance, August 2017

[12] See sections 582(b)(3), (c)(3), (d)(3), and (e)(3) of the FD&C Act (21 U.S.C. 360eee-1).

[13] See section 581(2) of the FD&C Act.

[14] See section 581(23) of the FD&C Act.

such that a verifiable credential itself can be easily ported from one repository to another without the need to reissue the credential. An example of a DID is did:eth:123454123412341236abcdef.

Decentralized Identifier Document

Also referred to as a ***DID document***, this is a document that is accessible using a verifiable data registry and contains information related to a specific decentralized identifier, such as the associated repository and public key information.

Digital Identity Wallet

At its core, an **identity wallet** is a software module, and optionally an associated hardware module, for securely storing and accessing private keys, link secrets, other sensitive cryptographic key material, and other private data used by an entity. Most wallets handle, present, and verify credentials and other kinds of information as well.

DSCSA

Drug Supply Chain Security Act[15]

Credential Issuer

A role an entity can perform by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder.

PI Verification Request

A GS1 standardized message presented to the manufacturer requesting verification of the Product Identification (NDC, Serial Number, Lot Number and Expiration Date) in accordance with the DSCSA. The manufacturer responds with a PI Verification Response.

PI Verification Response

A GS1 standardized message in response to a PI Verification Request. The manufacturer responds whether the Product Information (NDC, Serial Number, Lot Number and Expiration Date) was placed into commerce.

Product Information (PI)

The DSCSA defines Product Information as four attributes of a drug product; National Drug Code (NDC), Serial Number, Lot Number and Expiration Date.

Revocation Registry

Also referred to as a Revocation List. It is often useful for an issuer of verifiable credentials [VC-DATA-MODEL] to link to a location where a verifier can check to see if a credential has been revoked.

[15] See FDA website: https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa

Verifiable Credential

A set of one or more claims made by an issuer. A verifiable credential is a tamper-evident credential that has authorship that can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified.

Verifiable Presentation

Data derived from one or more verifiable credentials, issued by one or more issuers, that is shared with a specific verifier. A verifiable presentation is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. Certain types of verifiable presentations might contain data that is synthesized from, but does not contain, the original verifiable credentials (for example, zero-knowledge proofs).

Verification

The evaluation of whether a verifiable credential or verifiable presentation is an authentic and timely statement of the issuer or presenter, respectively. This includes checking that: the credential (or presentation) conforms to the specification; the proof method is satisfied; and, if present, the status check succeeds.

Verifier

A role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation for processing.

URI

A Uniform Resource Identifier, as defined by [RFC3986].

Exploring the Pilot

The pilot exercised the following scenarios:

Implementation of Trading Partners

- Identity Wallet Acquisition and Initialization
- Identity Credential Acquisition from Credential Issuer
- ATP Credential Acquisition from Credential Issuer
- Allowing VRS provider restricted access to Identity Wallet

Implementation of Credential Issuers

- Identity Wallet Acquisition and Initialization
- Connection of Identity Wallet to License Management system
- Connection of Identity Wallet to Credential Issuance Service

Issuance and Maintenance of Credentials

- Verifiable Company Identity Credential
    a. Due Diligence on company identity of Trading Partner
    b. Issuance of Verifiable Company Identity Credential
    c. Maintenance of Identity Credential
    d. Revocation of Identity Credential
- ATP Credential
    a. Due Diligence on Trading Partner License
    b. Issuance of ATP Credential
    c. Maintenance of ATP Credential
    d. Revocation of ATP Credential

PI Verification (e.g. Saleable Returns Verification)

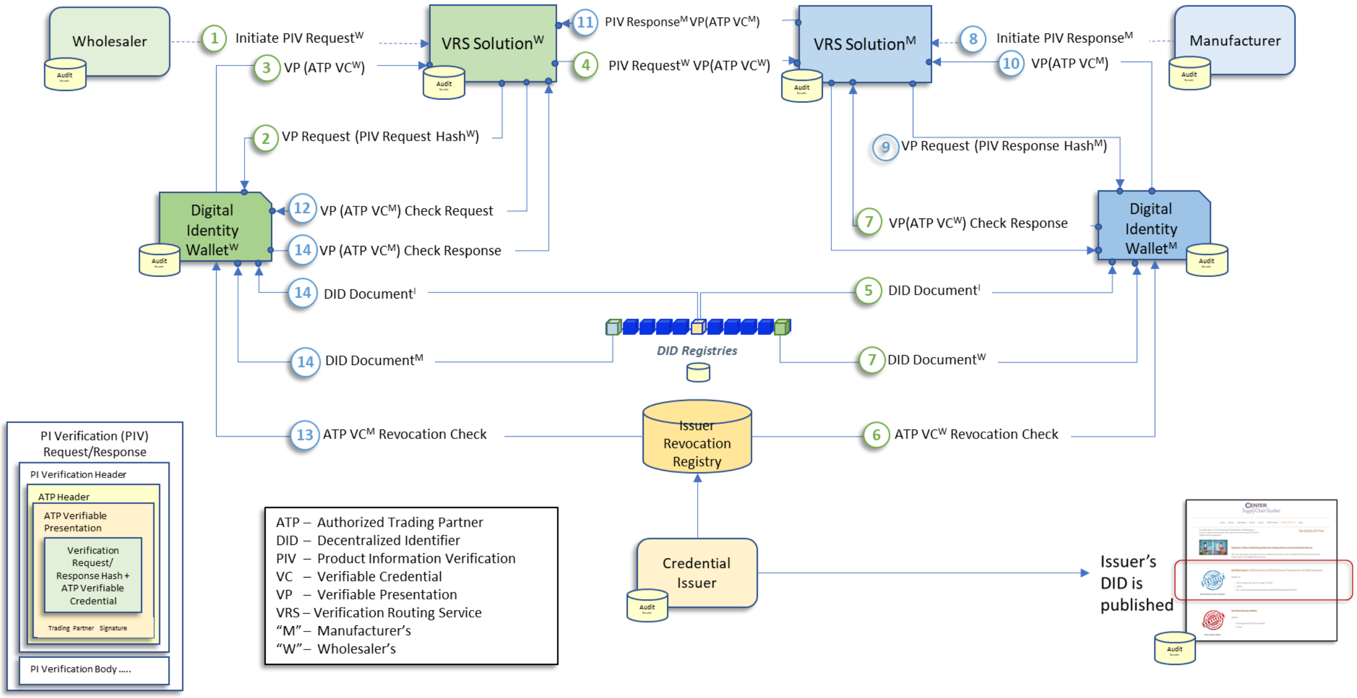
- **PI Verification with ATP Credentials**
    - PI Verification – Successful creation and verification of credentials on both sides, requestor and responder
    - PI Verification – Process of creating the credential of the requestor (Wholesaler) fails
    - PI Verification – Process of creating the credential of the responder (Manufacturer) fails
    - PI Verification – Wholesaler uses a revoked Credential
    - PI Verification – Manufacturer uses a revoked Credential

Audits and Investigations by Trading Partners

- Compliance officer audits the implementation Records
- Compliance officer audits the PI Verification Records
- Compliance officer investigates an ATP interaction that a Wholesaler initiated
- Compliance officer investigates an ATP interaction that a Manufacturer initiated

Figure 10 and the following process step descriptions depict the interaction among piloted roles. This scenario was repeated to allow each participating Trading Partner to experience and assess their role and the information that was available to them:

Pilot Role	Company
Wholesalers	AmerisourceBergen
	Cardinal Health
Manufacturers	Bristol Meyers Squibb
	Johnson & Johnson
	Novartis
VRS Solutions	SAP
	rfxcel
Issuer	Legisym
Digital Wallet Provider	Spherity


Wholesaler
Audit
1 Initiate PIV Request^{W}
3 VP (ATP VC^{W})
VRS Solution^{W}
11 PIV Response^{M} VP(ATP VC^{M})
4 PIV Request^{W} VP(ATP VC^{W})
VRS Solution^{M}
8 Initiate PIV Response^{M}
10 VP(ATP VC^{M})
Manufacturer
2 VP Request (PIV Request Hash^{W})
9 VP Request (PIV Response Hash^{M})
Digital Identity Wallet^{W}
12 VP (ATP VC^{M}) Check Request
14 VP (ATP VC^{M}) Check Response
7 VP(ATP VC^{W}) Check Response
Digital Identity Wallet^{M}
14 DID Document^{I}
5 DID Document^{I}
DID Registries
14 DID Document^{M}
7 DID Document^{W}
13 ATP VC^{M} Revocation Check
Issuer Revocation Registry
6 ATP VC^{W} Revocation Check
PI Verification (PIV) Request/Response
PI Verification Header
ATP Header
ATP Verifiable Presentation
Verification Request/ Response Hash + ATP Verifiable Credential
Trading Partner Signature
PI Verification Body .....
Credential Issuer
Issuer's DID is published

ATP – Authorized Trading Partner
DID – Decentralized Identifier
PIV – Product Information Verification
VC – Verifiable Credential
VP – Verifiable Presentation
VRS – Verification Routing Service
"M" – Manufacturer's
"W" – Wholesaler's

Figure 10 - Sample successful PI Verification using the ATP Verifiable Credential

The PI Verification Request **(follow the green #s in** Figure 10**):**

1. The Wholesaler initiates the PI Verification Request via their VRS Solution.
    a. Depending on the service provider's solution setup, this request may already contain the DID
2. The Wholesaler's VRS Solution:

   a. creates the PI Verification Request,
   b. calculates a hash value for it,
   c. either determines the DID of the requester or uses the DID transferred by the requester, and
   d. sends a request to the Wholesaler's Digital Identity Wallet to associate this hash with the Wholesaler's ATP Verifiable Credential.
3. The Wholesaler's Digital Identity Wallet:
   a. retrieves the Wholesaler's ATP Verifiable Credential,
   b. wraps it with a Verifiable Presentation (which includes the PI Verification Request Hash),
   c. signs the Verifiable Presentation using the Wholesaler's Private Key and
   d. sends the Verifiable Presentation back to the Wholesaler's VRS Solution in the form of a JSON Web Token (JWT).
4. The Wholesaler's VRS Solution:
   a. inserts the Verifiable Presentation (JWT) in the header of the PI Verification Request they created in step #2 and
   b. issues the verification request to the VRS ecosystem. The VRS executes the routing and forwards it to the Manufacturer's VRS Solution.
5. The Manufacturer's VRS Solution:
   a. checks the Wholesaler's PI Verification Request Hash in the Verifiable Presentation, to ensure that the Verifiable Presentation references the correct verification request and
   b. issues a Check Request of the Wholesaler's Verifiable Presentation and ATP Verifiable Credential to the Manufacturer's Digital Identity Wallet.
6. The Manufacturer's Digital Identity Wallet checks the Revocation Registry of the Wholesaler's ATP Verifiable Credential's Issuer to ensure the Wholesaler's ATP Verifiable Credential has not been revoked.
   a. this process can be executed offline in various modes. For example, all existing credentials could be checked for revocation in a batch job daily. This would eliminate the necessity to execute a revocation check during the PI verification.
7. Before sending a Check Response back to the Manufacturer's VRS Solution, the Manufacturer's Digital Identity Wallet also checks:
   a. the Wholesaler's signature in the Verifiable Presentation using the Wholesaler's Public Key found in the Wholesaler's DID Document,
   b. the Issuer's DID matches the Issuer's DID as published in a well-known location,
   c. the Issuer's signature in the Verifiable Credential using the Issuer's Public Key found in the Issuer's DID Document, and
   d. the Expiration Date of the Verifiable Credential.

At this point, the Manufacturer's VRS Solution is ensured of the identity of the Wholesaler and that the Wholesaler is a DSCSA Authorized Trading Partner and can process the PI Verification Request using the Manufacturer's ATP Verifiable Credential in a similar way as we saw the Wholesaler's VRS Solution.

The PI Verification Response **(follow the blue #s in** Figure 10**):**

This process follows along the same lines as the PI Verification Request steps above. They are included here to provide explicit steps and to reduce the chance of interpretation errors.

8. The Manufacturer's VRS Solution processes the Wholesaler's PI Verification Request based on the Manufacturer's instructions.
9. The Manufacturer's VRS Solution:
   a. creates the PI Verification Response,
   b. calculates a hash value for it,
   c. either determines the DID of the responder or uses the DID transferred by the responder, and
   d. sends a request to the Manufacturer's Digital Identity Wallet to associate this hash with the Manufacturer's ATP Verifiable Credential.
10. The Manufacturer's Digital Identity Wallet:
    a. retrieves the Manufacturer's ATP Verifiable Credential,
    b. wraps it with a Verifiable Presentation (which includes the PI Verification Response Hash),
    c. signs the Verifiable Presentation using the Manufacturer's Private Key and
    d. sends the Verifiable Presentation back to the Manufacturer's VRS Solution in the form of a JSON Web Token (JWT).
11. The Manufacturer's VRS Solution:
    a. inserts the Verifiable Presentation (JWT) in the header of the PI Verification Response they created in step #2 and
    b. issues the verification response to the VRS ecosystem. The VRS executes the routing and forwards it to the Wholesaler's VRS Solution.
12. The Wholesaler's VRS Solution:
    a. checks the Manufacturer's PI Verification Response Hash in the Verifiable Presentation, to ensure that the Verifiable Presentation references the correct verification response, and
    b. issues a Check Request of the Manufacturer's Verifiable Presentation and ATP Verifiable Credential to the Wholesaler's Digital Identity Wallet.
13. The Wholesaler's Digital Identity Wallet checks the Revocation Registry of the Manufacturer's ATP Verifiable Credential's Issuer to ensure the Manufacturer's ATP Verifiable Credential has not been revoked.
    a. this process can be executed offline in various modes. For example, all existing credentials could be checked for revocation in a batch job daily. This would eliminate the necessity to execute a revocation check during the PI verification.
14. Before sending a Check Response back to the Wholesaler's VRS Solution, the Wholesaler's Digital Identity Wallet also checks:
    a. the Manufacturer's signature in the Verifiable Presentation using the Manufacturer's Public Key found in the Manufacturer's DID Document,
    b. the Issuer's DID matches the Issuer's DID as published in a well-known location,
    c. the Issuer's signature in the Verifiable Credential using the Issuer's Public Key found in the Issuer's DID Document, and

d. the Expiration Date of the Verifiable Credential.

At this point, the Wholesaler's VRS Solution is ensured of the identity of the Manufacturer and that the Manufacturer is a DSCSA Authorized Trading Partner and can trust the PI Verification Response they have received.

Compliance Considerations

As complex as Figure 10 might seem, please note two points:

1. the Trading Partners are initiating a PI Verification Request or Response just as they would without the use of the piloted architecture. Nothing changes on a day-to-day basis.
2. The audit records provide a rich new set of information for supporting compliance proof.

The following may be helpful to the compliance team in your organization to verify the value of the architecture and as a starting conversation with technical experts who can verify these considerations after they examine the technical companion documents.

Roles and Minimum Responsibilities

Industry must:

- Agree on the due diligence or equivalent due diligence a Credential Issuer must perform in order to provide Trading Partners with Credentials.
- Require potential Credential Issuers to follow a minimum set of due diligence checks and maintain appropriate audit records and security.
- Require the entity publishing Issuer DIDs to maintain audit records and proper security.

Trading Partners:

- Maintain proper audit records which include correlation UUIDs in order to reproduce records associated with an individual PI Request / Response pair.
- Require the same of their VRS Providers and Digital Identity Wallet Providers.
- Take precautions to protect access to their Digital Identity Wallet and the Private Key established in their Digital Identity Wallet by ensuring that these are accessible only by the proper internal staff, using the same level of protection as used with DEA signing certificates.

VRS Solutions:

- Maintain proper audit records which include correlation UUIDs in order to reproduce records associated with an individual PI Request / Response pair.

Digital Wallets:

- Maintain proper audit records which include correlation UUIDs and Credential IDs in order to reproduce records associated with an individual PI Request / Response pair.
- Have mechanisms in place to detect fraudulent activity.

DID Registries:

- Maintain proper audit records in order to reproduce records associated with an individual DID.

Credential Issuers:

- Maintain proper audit records which include credential IDs in order to reproduce records associated with an individual PI Request / Response pair.
- To issue an Identity Credential, either:
  - Verify the Trading Partner's DEA Signing Certificate, or
  - Verify an industry agreed set of corporate documents.
- To issue an ATP Credential,
  - Verify the Trading Partner's Identity Credential, and
  - Verify that the Trading Partner holds the proper license or registration in accordance with the statute and FDA published guidances.

Well Known Site for Issuer DID Publication:

- To verify the Issuer's digital signature in a Verifiable Credential, a Trading Partner's Digital Wallet must use the Issuer's Public Key associated with the Private Key that the Issuer used to sign the Verifiable Credential. The Public Key can be found in the Issuer's DID Document in a DID Registry of the Issuer's choice. As with all DIDs, the Issuer's DID (found in the Verifiable Credential) acts as an address to the DID Document and the Issuer's Public Key.
- The Issuer's DID isused to determine the location of the Issuer's DID Document where their public key is maintained.
- The Issuer's DID must be published in a location known to all Digital Wallet providers
- The entity maintaining the "well known site for Issuer DID Publication" must:
  - Maintain proper audit records of changes to the published DIDs.
-

Private Key Management and Protection

#2 & #3 and #9 & #10: As the signatures created on behalf of the Trading Partner binds that Trading Partner, the keys must be protected. To this end, the following have been implemented in the pilot:

1. Only the Trading Partners (their designated representatives) have access to know the Private Key used for signing.

2. The Digital Wallet Provider does not have visibility to the Trading Partner’s Private Key.
3. Using the Digital Wallet, the Trading Partner can change the Private Key (rotate keys) in the wallet and its associated Public Key in the Trading Partner’s DID Document.

Mitigating nefarious or accidental PI Requests or PI Responses

#2 & #3 and #9 & #10: The Trading Partner’s VRS Solution is given limited access to the Trading Partner’s Digital Identity Wallet. That access is given by the Trading Partner itself. Also, both the VRS Solution and the Digital Identity Wallet keeps an audit record of the Signing requests / responses along with a Universally Unique Identifier (UUID) that allows the Trading Partner to match requests and responses during an audit or investigation.

#4 and #11: The use of a Verification Presentation over the Verifiable Credentials ensures that the Trading Partner permissioned the use of their Verifiable Credential for this current PI Request or PI Response only. Including the PI Request Hash and the Trading Partner signature or the PI Response Hash and the Trading Partner signature in the Verifiable Presentation, along with audit records at each step, mitigates the risk of Verifiable Credentials being used without the owning Trading Partner’s knowledge.

Value of the Verifiable Presentation / Verifiable Credentials for Compliance

The value of the Verifiable Presentation / Verifiable Credential combination is determined by:

1. The due Diligence performed by the Credential Issuer.
2. The upkeep and verification of the Revocation Registry.
3. The verifications performed by the Digital Identity Wallet.
4. The wrapping of the ATP Verifiable Credential in a Verifiable Presentation that includes the PI Verification Request / Response hash and Trading Partner Digital Signature.

Verifying the Identity and ATP Status of the Trading Partner

# 5, #6 & #7 and #12, #13 & #14: The heart of the pilot: can the ATP Status of an unknown DSCSA defined Trading Partner be cryptographically verified? This job is split between the Trading Partner’s VRS Solution and the Trading Partner’s Digital Identity Wallet which makes use of the opposite Trading Partner’s DID Document, and the Verifiable Credential’s and Issuer’s Revocation Registry.

The use and configuration of the Trading Partner DID, DID Document, Public and Private Key management, Issuer due diligence and Revocation Registry, Verifiable Presentation and Verifiable Credential embedded in the header of the PI Request and PI Response, allow for the VRS Solution and the Trading Partner Digital Identity Wallet to perform cryptographically sound checks to assess the validity of the presented identity and ATP Status of the opposite Trading Partner.

Audit and Investigation support

# 1 - #14: All steps include the creation and retention of appropriate audit records. These records include the UUID used throughout the system to connect a full round trip from PI Inception (#1) through the final check of credentials (#14).

# 6 - #13: Be aware that there may be a delay between when the FDA or State Boards of Pharmacies make a license or registration determination, and when the information is published so that the Credential Issuer can affect a change in the Credential Revocation Registry. This will be evident when the license revocation date is earlier than the published date (on the regulator's site) and the Credential Revocation Date.

Performance enhancement

# 6 - #13: Credential Revocation Checks: The FDA and State Boards of Pharmacy update the license and registration information on a variety of schedules. These schedules vary from daily to weeks, to months. The Credential Issuer checks the status of licenses and registrations according to those schedules in order to detect a potential revocation trigger. Therefore, Revocation Registries remain static at least for 24-hour periods. Digital identity Wallets may copy revocation registries daily and access their local copy to increase performance.

Business Operations Considerations

As complex as Figure 10 might seem, please note that the Trading Partners are initiating a PI Verification Request or Response just as they would without the use of the piloted architecture. Nothing changes on a day-to-day basis.

The following may be helpful to the Business Operations team in your organization to verify the value of the architecture and as a starting conversation with technical experts who can verify these considerations after they examine the technical companion documents.

Roles and Minimum Responsibilities

VRS Solutions:

- Maintain proper audit records which include correlation UUIDs in order to reproduce records associated with an individual PI Request / Response pair.
- Check that the content of Verifiable Credentials received match the identity of the Trading Partner represented in the PI Request / PI Response Body.
- Check that the Credentials of Trading Partners you support are not revoked. This does not need to be performed for each transaction; however, it should be performed in cadence with the Credential Issuers publication schedule.

Digital Wallets:

- Maintain proper audit records which include correlation UUIDs in order to reproduce records associated with an individual PI Request / Response pair.
- Have mechanisms in place to detect fraudulent activity.

DID Registries:

- Maintain proper audit records which include correlation UUIDs in order to reproduce records associated with an individual PI Request / Response pair.

Credential Issuers:

- Maintain proper audit records which include correlation UUIDs in order to reproduce records associated with an individual PI Request / Response pair.
- Publish a Revocation Registry update cadence.

Well Known Site for Issuer DID Publication:

- To verify the Issuer's digital signature in a Verifiable Credential, a Trading Partner's Digital Wallet must use the Issuer's Public Key associated with the Private Key that the Issuer used to sign the Verifiable Credential. The Public Key can be found in the Issuer's DID Document in a DID Registry of the Issuer's choice. As with all DIDs, the Issuer's DID (found in the Verifiable Credential) acts as an address to the DID Document and the Issuer's Public Key.
- The Issuer's DID isused to determine the location of the Issuer's DID Document where their public key is maintained.
- The Issuer's DID must be published in a location known to all Digital Wallet providers
- The entity maintaining the "well known site for Issuer DID Publication" must:
- Maintain proper audit records of changes to the published DIDs.

Confidentiality

#2 & #3 and #9 & #10: To isolate the Digital Wallets from having knowledge of the PI Verification Request / Response details, the Digital Wallets are passed a hash of the PI Request or PI Response to be included in the Verifiable Presentation. A hash is a value calculated using a set of data in order to later prove that the data was not altered. For the pilot we used what is referred to as a SHA256 hash algorithm[16] on the data set of the GTIN, Serial Number, Lot Number and Expiration Date.

Private Key Management and Protection

#2 & #3 and #9 & #10: As the signatures created on behalf of the Trading Partner binds that Trading Partner, the keys must be protected. To this end, the following have been implemented in the pilot:

1. Only the Trading Partners (their designated representatives) have access to know the Private Key used for signing.
2. The Digital Wallet Provider does not have visibility to the Trading Partner's Private Key.

[16] https://en.wikipedia.org/wiki/SHA-2

3. Using the Digital Wallet, the Trading Partner can change the Private Key (rotate keys) in the wallet and its associated Public Key in the Trading Partner's DID Document.

Mitigating nefarious or accidental PI Requests or PI Responses

#2 & #3 and #9 & #10: The Trading Partner's VRS Solution is given limited access to the Trading Partner's Digital Identity Wallet. That access is given by the Trading Partner itself. Also, both the VRS Solution and the Digital Identity Wallet keeps an audit record of the Signing requests / responses along with a Universally Unique Identifier (UUID) that allows the Trading Partner to match requests and responses during an audit or investigation.

#4 and #11: The use of a Verification Presentation over the Verifiable Credentials ensures that the Trading Partner permissioned the use of their Verifiable Credential for this current PI Request or PI Response only. Including the PI Request Hash and the Trading Partner signature or the PI Response Hash and the Trading Partner signature in the Verifiable Presentation, along with audit records at each step, mitigates the risk of Verifiable Credentials being used without the owning Trading Partner's knowledge.

Verifying the Identity and ATP Status of the Trading Partner

# 5, #6 & #7 and #12, #13 & #14: The heart of the pilot: can the ATP Status of an unknown DSCSA defined Trading Partner be cryptographically verified? This job is split between the Trading Partner's VRS Solution and the Trading Partner's Digital Identity Wallet which makes use of the opposite Trading Partner's DID Document, and the Verifiable Credential's and Issuer's Revocation Registry.

The use and configuration of the Trading Partner DID, DID Document, Public and Private Key management, Issuer due diligence and Revocation Registry, Verifiable Presentation and Verifiable Credential embedded in the header of the PI Request and PI Response, allow for the VRS Solution and the Trading Partner Digital Identity Wallet to perform cryptographically sound checks to assess the validity of the presented identity and ATP Status of the opposite Trading Partner.

Audit and Investigation support

# 1 - #14: All steps include the creation and retention of appropriate audit records. These records include the UUID used throughout the system to connect a full round trip from PI Inception (#1) through the final check of credentials (#14).

# 6 - #13: Be aware that there may be a delay between when the FDA or State Boards of Pharmacies make a license or registration determination, and when the information is published so that the Credential Issuer can affect a change in the Credential Revocation Registry. This will be evident when the license revocation date is earlier than the published date (on the regulator's site) and the Credential Revocation Date.

Performance Consideration

# 6 and #13: Although the technology, processes and architecture add up to a trustworthy system, Manufacturers may require a check of information by Business Operations or Compliance staff for PI Verification originated from DSCSA defined Trading Partners that are not actual Trading Partners in the business sense of the term. Systems should accommodate for a longer time to pass for these occasions. A strategy to not delay transactional processing could be to initiate an initial PI Request for a product from each Manufacturer's line of products that are purchased.

Technical Considerations

The following companion documents will be more informative to the reader seeking technical details of the pilot:

- Architecture Handbook
- ATP Credentialing - Audit Requirements
- ATP Credentialing Pilot – Security Analysis
- API Documentation

The following are technical considerations of the sample PI Verification process in Figure 10.

How Trading Partners initiate PI Requests and PI Responses

#1 & #8: It is expected that Trading Partners may initiate PI Requests and PI Responses from within their VRS Solution either by signing in and initiating them directly or by setting configuration. Alternately, the initiation could occur via electronic message from the Trading Partner's internal system.

Confidentiality

#2 & #3 and #9 & #10: To isolate the Digital Wallets from having knowledge of the PI Request / Response details, the Digital Wallets are passed a hash of the PI Request or PI Response with the Verifiable Presentation and signed. The hash is calculated using the SHA256 algorithm over the DSCSA defined Product Information (GTIN, Serial Number, Lot Number and Expiration Date).

Private Key Management and Protection

#2 & #3 and #9 & #10: As the signatures created on behalf of the Trading Partner bind that Trading Partner, they must be protected. To this end, the following has been implemented in the pilot:

1. Only the Trading Partners (their designated representatives) have access to know the Private Key used for signing.
2. The Digital Wallet Provider does not have visibility to the Trading Partner's Private Key.
3. Using the Digital Wallet, the Trading Partner can change the Private Key (rotate keys) in the wallet and its associated Public Key in the Trading Partner's DID Wallet.

Mitigating nefarious or accidental PI Requests or PI Responses

#2 & #3 and #9 & #10: The Trading Partner's VRS Solution is given limited access to the Trading Partner's Digital Identity Wallet. That access is given by the Trading Partner itself. Also, both the VRS Solution and the Digital Identity Wallet keep an audit record of the Signing requests / responses along with a Universally Unique Identifier (UUID) that allows the Trading Partner to match requests and responses during an audit or investigation.

#4 and #11: The use of a Verification Presentation over the Verifiable Credentials ensures that the Trading Partner permissioned the use of their Verifiable Credential for this current PI Request or PI Response only. Including the PI Request Hash and the Trading Partner signature or the PI Response Hash and the Trading Partner signature in the Verifiable Presentation along with audit records at each step mitigates the risk of Verifiable Credentials being used without the owning Trading Partner's knowledge.

Verifying the ATP Status

#6 & #7 and #13 & #14: Once a Verifiable Credential and Verifiable Presentation are received by a VRS provider (or directly by a Trading Partner in some cases), the information they contain can be cryptographically verified. In addition, attributes in the Verifiable Credential and the Verifiable Presentation can be checked against other data the Trading Partner already has possession of.

1. The Universally Unique ID (UUID) in the verifiable presentation must match the UUID in the PI Verification Request or Response.
2. The PI Verification Request or Response Hash value must match a Hash value calculated from the PI Verification Request or Response itself (without the XATP Header containing the Verifiable Presentation and ATP Verifiable Credential).
3. The Trading Partner Digital Signature must match a signature created using the Private Key associated with the Company DID found in the ATP Credential. This shows that the Trading Partner identified by the Company DID did execute the PI Verification Request or Response. The check is accomplished with the Public Key associated with the Company DID, which can be found by using the Company DID to retrieve the DID Document as specified by W3C standards.
4. The ATP Verifiable Credential must not be revoked. This can be checked by accessing the Issuer's Revocation Registry and ensuring the Credential ID is not listed as "revoked".
5. The ATP status of the Trading Partner is established by the presence of the ATP Verifiable Credential.
6. The Credential Type must match the action taken by the Trading Partner.
    1. Credential Type must be "W" if this is a PI Verification Request for a Saleable Return.
    2. Credential Type must be "W" or "D" if this is a PI Verification Request for an Investigation (future requirement).
    3. Credential Type must be "M" if this is a PI Verification Response.
7. The Company Name is the Trading Partner's corporate entity name that the ATP Verifiable Credential Issuer verified prior to issuing the credential.
8. The GLN is an optional attribute and will be used to explore usage of a future GLN credential.

9. The Issuer DID must be a “well known DID” by being published by a trusted source that has certified the Issuer and verified the DID.

10. The Issuer Digital Signature must match a signature created using the Private Key associated with the Issuer DID found in the ATP Credential. This shows that the Entity identified by the Issuer DID did complete the required due diligence for the Identity Credential and the ATP Credential issued to the Entity identified by the Company DID. The check is accomplished with the Public Key associated with the Issuer DID, which can be found by using the Issuer DID to retrieve the DID Document as specified by W3C standards.

Disclaimer

Except as may be otherwise indicated in specific documents within this publication, you are authorized to view documents within this publication, subject to the following:

1. You agree to retain all copyright and other proprietary notices on every copy you make.
2. Some documents may contain other proprietary notices and copyright information relating to that document. You agree that the Center for Supply Chain Studies has not conferred by implication, estoppels, or otherwise any license or right under any patent, trademark, or copyright (except as expressly provided above) of the Center for Supply Chain Studies or of any third party.

This publication is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Any Center for Supply Chain Studies publication may include technical inaccuracies or typographical errors. The Center for Supply Chain Studies assumes no responsibility for and disclaims all liability for any errors or omissions in this publication or in other documents which are referred to within or linked to this publication. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

The Center for Supply Chain Studies shall not be liable for any consequential, special, indirect, incidental, liquidated, exemplary, or punitive damages of any kind or nature whatsoever, or any lost income or profits, under any theory of liability, arising out of the use of this publication or any content herein, even if advised of the possibility of such loss or damage or if such loss or damage could have been reasonably foreseen.

No Liability for Consequential Damage

In no event shall the Center for Supply Chain Studies or anyone else involved in the creation, production, or delivery of the accompanying documentation be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other loss) arising out of the use of or the results of use of or inability to use such documentation, even if the Center for Supply Chain Studies has been advised of the possibility of such damages.

Contact information

Bob Celeste, Founder

Center for Supply Chain Studies
www.c4scs.org
P: 215.584.7374
E: rceleste@c4scs.org