SPHERITY

Credentialing for U.S. Pharmaceutical Dispensers in support of Drug Supply Chain Security Act (DSCSA) compliance

Utilizing Verifiable Credentials to authenticate Authorized Trading Partner Status

Proof-of-Concept
Public Report

DOCUMENT HISTORY

Version	Date	Changes
1.0	2/1/22	First public version created

TABLE OF CONTENTS

SCOPE OF THIS POC

The Open Credentialing Initiative (OCI) has developed an electronic and interoperable solution for Authorized Trading Partners (ATP). This credential-based solution was developed together with manufacturers, wholesalers, VRS, and credentialing and digital identity solutions providers. The first use case addressed by OCI is saleable returns verification. More information on the respective industry-wide pilot can be found on the OCI website. The business requirements of Dispensers (e.g. suspicious product verification) were considered but not specifically addressed in the ATP pilot. Hence, Spherity together with fellow OCI members Legisym and RxScan decided to run a Dispenser proof-of-concept (PoC) as an extension to the original ATP pilot.

The Dispenser PoC focused on the use case of pharmaceutical product identifier (PI) verification. The objective of the PoC was to demonstrate that solution providers serving Dispensers are able to use the OCI architecture and provide affordable credentialing services to their customers. The key challenge was to clarify how Dispensers can be onboarded to receive both an Identity and ATP Credential and how to manage their credentials using a digital wallet.

GLOSSARY

Application Programming Interface (API)

An API is an intermediary layer between computers or computer programs based on defined rules for such connections.

Authorized Trading Partner (ATP)

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. DSCSA includes definitions for 'authorized' and 'trading partner' 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.

Digital Wallet

At its core, a digital wallet (aka 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.

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.

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.

LEGAL REQUIREMENTS FOR DISPENSERS

Under the Drug Supply Chain Security Act (DSCSA), beginning November 27, 2023, Dispensers are required to electronically engage in:

1. **Interoperable Medication Information Exchange.**

   Trading Partners must exchange required Transaction Information (TI) and Transaction Statements (TS) in a secure, electronic, and interoperable manner, and the TI must include the Product Identifier at the package level.

2. **Interoperable Medication Product Identifier Verification.**

   Trading Partners must be able to verify the Product Identifier on a package or sealed homogeneous case in a secure, electronic, and interoperable manner.

3. **Interoperable Medication Ownership History Tracing.**

   Trading Partners must maintain secure, electronic, and interoperable systems and processes to provide TI and TS in response to a request for these and to promptly facilitate gathering of the information necessary to produce the TI trail for each transaction tracing back to the manufacturer.

Since these requirements involve parties that very often do not have a commercial relationship, there is a need for these parties to be able to verify electronically that they are talking to parties

A. who are who they say they are; and
B. who are allowed to engage in these types of communications.

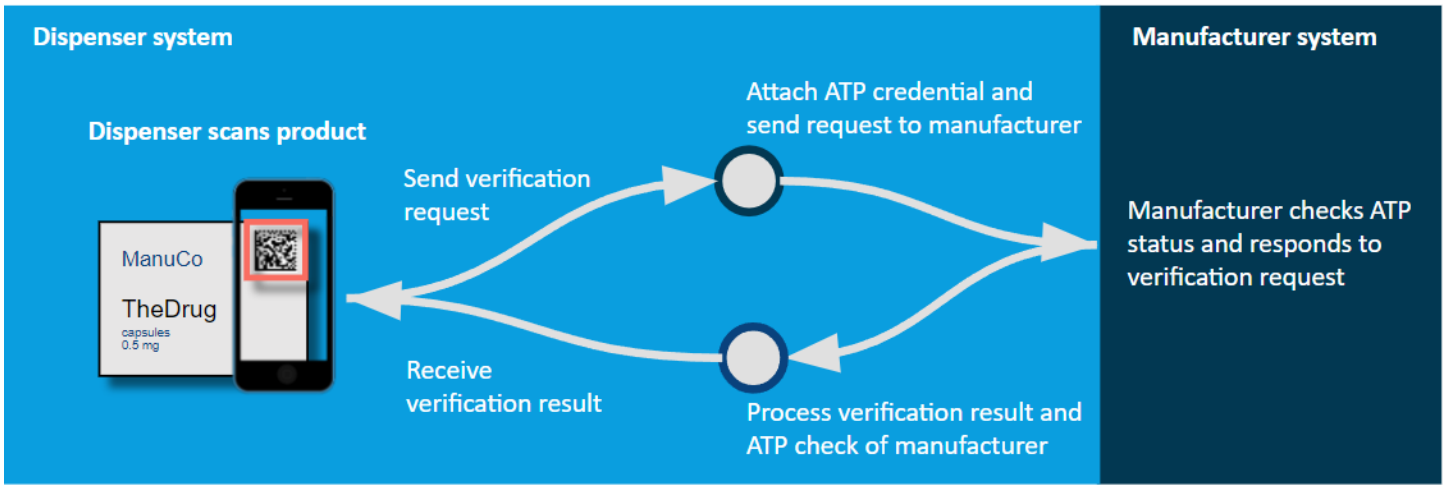
INTEROPERABLE MEDICATION PRODUCT IDENTIFIER VERIFICATION

A Dispenser has multiple options for meeting requirements to verify a medication product that is suspicious. The table below compares a manual product verification with an automated solution. The latter is enabled by OCI´s architecture using credentialing.

Method	Process	Challenge	Impact for dispenser
Manual	Contact • supplier's sales representative • supplier's service hotline • manufacturer's service hotline	• Who is the right person to call or email? • What information do I need to provide? • When will I get a response? • Do I need to return the medication to verify it? • Are other medications affected? • What effect will this have on patient care?	• Expected response time of 2-3 days. • Patient care may be negatively affected and their confidence and loyalty diminished when medication cannot be provided timely. • No sales when medication verification results are unclear and further inventory is affected.
Electronic	Dispenser scans product with an app or existing scanning device (see graphic below)	• Adoption of electronic solution by service providers • Onboarding of Dispensers	• Immediate response (max. 10 sec) ensures shorter process interruption and enables quicker dispensing (or quarantining) • Simpler, faster means of complying with DSCSA requirements • Automated electronic record-keeping for audits

Electronic system enables real-time response after scanning a suspicious product

This is how it works:



The solution is designed to be compatible with existing Data or Warehouse Management Systems offered by solution providers such as OCI member RxScan. These service providers are able to integrate via API with the Credential Issuer and Digital Wallet Provider. In order to route the PI Verification Request to the respective responder, a Verification Routing Service (VRS) is required.

VERIFICATION ROUTING SERVICE INTEGRATION

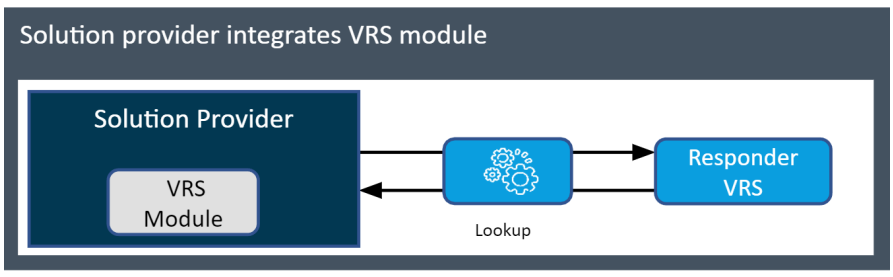
After scanning the product, a method is required to find the respective manufacturer. This is facilitated by VRS. The technical VRS integration in this context was not tested as part of the original ATP pilot phase. Nevertheless, the utilized GS1 Lightweight Standard for Product Verification Messages can also be employed to enable VRS to route Dispenser-triggered requests regarding suspicious products.

There are fundamentally two options for VRS providers to interact with service providers that enable Dispensers to scan products and run verifications:

- Direct integration using a VRS module or
- Indirect process by sending PI Message to VRS

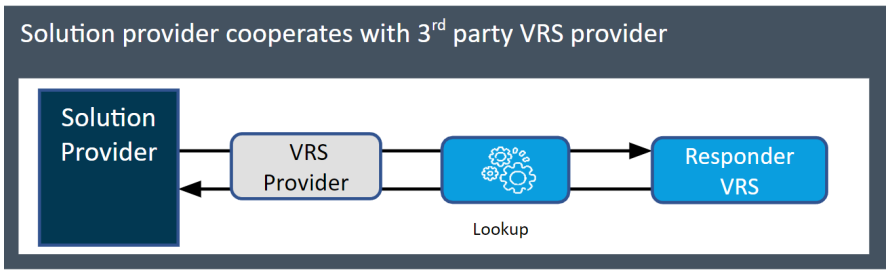
Direct Integration

The product scan service provider integrates in the backend a software module with all VRS features. This enables the service provider to create a GS1 Standardized PI Message and send it directly - via routing - to the responder.



Indirect Process

The product scan service provider sends the PI Message through an external VRS to get the message to the correct responder. This enables a simpler and quicker implementation.



OCI SOLUTION ARCHITECTURE FOR DISPENSERS

OCI PoC participants examined how Dispensers can adopt credentialing in a lean, simple and affordable way. This is particularly relevant for the onboarding of small community pharmacies and retail chains.

1. **Integrations for Existing Service Providers**

   OCI maintains open APIs that enable Dispensers' service providers to integrate with Digital Wallet Providers and Credential Issuers.

2. **Dispenser Onboarding**

   OCI ensures that small, medium, and large companies benefit from consistent and excellent user experience.

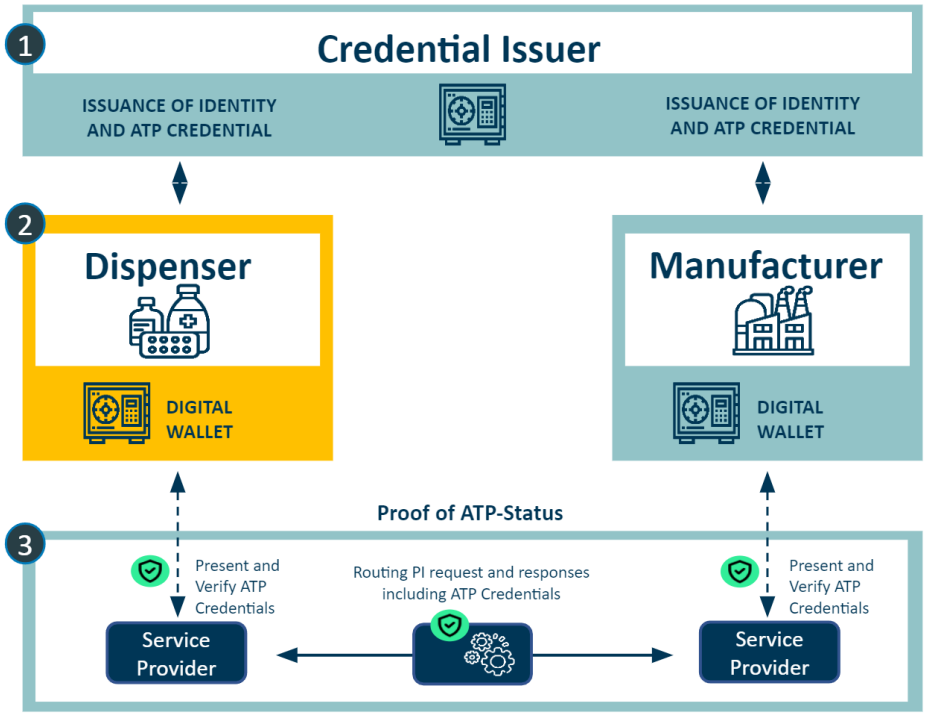
3. **Usage of Credentials for PI Verification**

   OCI specifications ensure that Dispensers share their own authorized status and verify others in digital interactions.

High Level Architecture and Process

This high level architecture describes how Dispensers can use their digital wallet and credentials to interact with other ATP. The Dispenser has access to a digital wallet user interface to perform the onboarding process, manage users, and to use the provided dashboard to investigate all interactions with ATPs.

The technical integration of credentialing into the suspicious product verification process is arranged between the VRS or dispenser's service provider and the Digital Wallet Provider. The Dispenser only uses the provided user interface and has no technical integration effort.



Step 1: Dispenser Acquires Identity and ATP Credential

- Credential Issuer verifies the digital identity and license status of each Dispenser
- Simple onboarding via system integration to existing service provider of Dispenser
- Issuance of Identity and ATP Credentials to Dispensers

Step 2: Dispenser Manages Own Credentials

- Dispenser has access to their own digital wallet to manage users and credentials
- Dispenser has access to a dashboard with all ATP interactions

Step 3: Dispenser Uses and Verifies ATP Credential in Product Verifications

- VRS (module) manages the PI Message requests and responses
- Solution provider uses API to create a Verifiable Presentation (VP) of the ATP Credential used in the PI
- VRS or dispenser's solution provider verifies incoming ATP credentials by sending them to the digital wallet

Dispenser Onboarding

The PoC group examined the onboarding process for Dispensers in detail. In conclusion, Dispensers are able to use the same onboarding process designed in the ATP Credentialing architecture and extensively tested in the original ATP pilot. Before acquiring the Identity Credential, a Dispenser needs to go through a due diligence process. After successful proof of identity, the Credential Issuer issues an ATP Credential based on a valid State-issued license. The detailed process and conformance criteria are described in the Credential Issuer Conformance Criteria published by OCI on oc-i.org.

COMMERCIAL IMPLICATIONS

This PoC demonstrates that existing systems and processes can be leveraged to enable affordable solutions for the adoption of OCI-standardized credentialing by Dispensers.

NEXT STEPS

Following completion of this technical evaluation by all project participants, the next phase will involve a technical prototype. This prototype will be tested by selected pharmacies.

STATEMENTS FROM POC PARTICIPANTS AND OBSERVERS

Max Peoples, Owner RxScan

Our goal was to simplify the credentialing of Dispensers, to make the process as intuitive as possible and with it requiring the least amount of time to complete. Through everyone's efforts we believe this has been accomplished.

David Kessler, President & Co-Owner at Legisym, LLC

By enabling the use of DEA Signing Certificates, OCI can leverage within just a few minutes this fast, dependable method that local pharmacies and small dispensers are already commonly familiar with – keeping the onboarding process simple and secure.

Georg Jürgens, Manager Industry Solutions at Spherity

Integrating credentialing into existing warehouse or ERP solutions used by Dispensers is key to enabling industry adoption. With OCI, we standardize the onboarding processes and interfaces to connect with Digital Wallets that are required to establish trust in digital identities and credentials of Dispensers.

Bob Celeste, C4SCS Founder

This PoC was an important step in establishing the use of W3C standard verifiable credentials by the DSCSA Dispenser community.

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 Spherity 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 Spherity 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 noninfringement. Any Spherity publication may include technical inaccuracies or typographical errors. The Spherity 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 Spherity 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 Spherity 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 Spherity has been advised of the possibility of such damages.

Contact information

Please send any feedback or enquiries to atp@spherity.com.