PDG Blueprint & OCI Conformance: Meeting the Requirements for Credentialing & Trading Partner Authentication

Introduction

The Partnership for DSCSA Governance (PDG) has released a Foundational Blueprint for 2023 Interoperability as part of its mission to develop, advance, and sustain the effective and efficient model for interoperable tracing and verification of prescription pharmaceuticals as required by the DSCSA. The Blueprint establishes that Authorized Trading Partner (ATP) authentication is critical to these efforts, and establishes requirements for verifying authorized status as well as identity proofing.

OCI is a collaborative, non-profit initiative formed by a group of trading partners, solution providers, and standards organizations to support the industry in adopting credentialing and digital wallet technologies. The initiative started in 2019 with a project supporting DSCSA compliance for ATP requirements. Our industry-wide pilot included the Healthcare Distribution Alliance (HDA), 2 VRS providers, 5 trading partners, 1 wallet provider, and 1 credential issuer.

In support of PDG's work, and in the spirit of greater interoperability, OCI has compiled a number of published resources. This document serves to bridge the compliance requirements and business requirements outlined in the "Support Credentialing and Trading Partner" section of PDG's Foundational Blueprint for 2023 Interoperability, and those outlined in the OCI's Conformance Criteria.

Resources:

- PDG Foundational Blueprint for 2023 Interoperability ("PDG Blueprint")
- OCI Credential Issuer Conformance Criteria ("OCI CICC")
- OCI Digital Wallet Conformance Criteria ("OCI DWCC") [DRAFT]

Authorized Trading Partner (ATP) Status

Requirements 1–5 are each specific to a single ATP type: manufacturers, repackagers, virtual manufacturers, wholesale distributors, and dispensers. In each case, the credential must:

- enable trading partners to confirm the authorized status of a credential holder for the purposes of tracing and/or verification; and
- leverage relevant state and federal registration and licensure databases to confirm current valid status.

The OCI CICC meets these requirements, including processes to validate authorized status and perform due diligence based on the definitions of these roles in the DSCSA statute and the PDG Blueprint. OCI and PDG are both in agreement that Identity and ATP Credentials must be validated within the ecosystem (as mentioned in Requirement-Cred-001, 002, 003, 004, 005 of the Blueprint); however, in the OCI ecosystem, this condition is aligned with the Digital Wallet Provider, not the Credential Issuer. In particular, these requirements are covered under OCI CICC 5. Authorized Trading Partner (ATP) Credential Due Diligence. (It should be noted that while virtual manufacturers are not included in the current OCI CICC, there are no technical barriers to the adoption of Requirement 3.)

Requirement 6 requires a "robust exceptions handling process for specific distribution or dispensing sites that are either permanently or temporarily not authorized." This requirement is met by OCI CICC 6.3 Identity Credential Monitoring and Expiration, OCI CICC 6.4 Triggers for Identity Credential Revocation/Recertification, OCI DWCC 4.1.9 Credential Revocation, and OCI DWCC 4.4 OCI Non-functional Wallet Features.

Audit Trail

Requirement 7 requires "a record of each confirmation of authorized status, the source documentation utilized to validate authorized status, including any changes to source documentation (e.g., renewed license, revoked license), and a record of modifications, if any, that are made to the record of a trading partner's authorized status (e.g., grace period exemptions). This information shall be maintained in a manner that would allow for periodic and/or impromptu inspections." This requirement is met by OCI CICC 6.5. Identity Credential Audit Trail, 6.8 ATP Credential Audit Trail, and OCI DWCC 4.3 OCI Functional Wallet Features. OCI CICC specifies the Credential Issuer records data from the original issuance of a credential, any change or modification, and the most recent periodic check.

Validation of ATP Credential Source Documentation

Requirements 8 and 9 requires that state regulators and FDA be able to push alerts and updates to licensure/registration information, and that regulators may therefore opt in to push updates or may continue with their current systems and processes. As noted earlier, OCI CICC already draws authorized status confirmation from the current systems and processes made available by state and federal agencies. The OCI is open to discussion with state and federal agencies in the event that push updates are desired.

Requirement 10 requires that authorized status verifications be performed upon expiry of a current license, as well as weekly or (in the case of state databases) as frequently as the database is updated. This requirement is met by OCI CICC 6.3 Identity Credential Monitoring and Expiration and 6.6 ATP Credential Monitoring and Expiration and exceeded by OCI CICC 6.4 Triggers for Identity Credential Revocation/Recertification and 6.7 Triggers for ATP Credential Revocation/Recertification.

Requirement 11 requires revocation of a credential within 4 hours of learning that the conditions of the credential are no longer met. In conformance with PDG Requirement 7, which allows for "grace period" exemptions, OCI CICC 6.4 Triggers for Identity Credential Revocation/Recertification and 6.7 Triggers for ATP Credential Revocation/Recertification currently allow for a grace period of 30 days whereby the Credential Owner may provide an alternate license or otherwise resolve the issue. Nonetheless, a 4-hour revocation requirement may be readily met.

Requirement 12 requires a "valid and secure technical mechanism to prove and verify the ATP status of the organization" which must "be interoperable with all other technical mechanisms within the PDG ecosystem."

This technical mechanism is outlined in the OCI DWCC, leveraging recognized National Institute of Standards and Technology (NIST) guidelines, W3C specifications for Verifiable Credentials and Decentralized Identifiers, and the GS1 Lightweight Messaging Standard. Member organizations of the OCI have successfully tested and deployed credentialing for the purposes of product verification alongside leading VRS and other software providers. The OCI Digital Wallet providers proved interoperability by verifying each other's credentials. Testing and deployment for the purposes of tracing is currently underway.

Requirement 13 requires that this technical mechanism "shall accommodate proxy or delegated use as designated by the credentialed entity." This requirement is met by OCI DWCC 4.3 OCI Functional Wallet Features.

Organizational Identity

Requirement 14 requires that Accredited Credential Issuers must verify one of three sets of information to establish the existence and identity of an organization. This requirement is met by OCI CICC 4. Evidence for Identity proofing based on NIST IAL2.

Moreover, the OCI has articulated a more in-depth validation of these requirements, backed by NIST Identity Assurance Level 2 (IAL2) guidelines. For example, the first set of supporting documentation identified in the requirement shall only suffice if the IRS EIN Letter meets certain threshold requirements (see section 4.4.4), as Articles of Incorporation and DUNS Numbers are publicly searchable and therefore considered to be weak evidence under NIST IAL2.

Requirement 15 is met by the OCI CICC, as it allows for discretion by Accredited Credential Issuers.

Requirement 16 requires that a credential not be issued if the supporting document appears to be invalid. This requirement is met by OCI CICC 4. Evidence for Identity proofing based on NIST IAL2.

Requirement 17 requires the issuance of a "valid and secure technical mechanism to prove and verify the identity of the organization." See the earlier response to Requirement 12.

Requirement 18 requires that this technical mechanism "shall accommodate proxy or delegated use as designated by the credentialed entity." See the earlier response to Requirement 13.

Audit Trail

Requirement 19 requires "a record of each confirmation of authorized status (i.e., a valid Accredited Credential Issuer-issued technology mechanism in combination with the organization's technology mechanism), the source documentation utilized to validate authorized status, including any changes to source documentation, and a record of modifications, if any, that are made to the record of a trading partner's authorized status (e.g., mergers, acquisitions). This information shall be maintained in a manner that would allow for periodic and/or impromptu inspections." This requirement is met by OCI CICC 6.5. Identity Credential Audit Trail and OCI DWCC 4.3 OCI Functional Wallet Features.

Conclusion

With less than two years until the DSCSA deadline, the industry is looking to PDG and the OCI ecosystem to advance the interoperability required by the statute and envisioned by the PDG Blueprint. OCI looks forward to working closely with PDG, together charting a clear path to 2023 interoperability.