Partnership for DSCSA Governance (PDG) Foundational Blueprint for 2023 Interoperability

Chapter 6: DSCSA Credentialing and User Authentication Functional Design

Version 1.2
July 15, 2023

Table of Contents

Table of Figures

Chapter 6: DSCSA Credentialing and User Authentication Functional Design

Chapter 1 defines requirements and recommendations for credentialing trading partners to ensure they are "authorized," as required by the DSCSA, and identity-proofed for PI Verification and TI Tracing processes within the PDG-defined Enhanced Drug Distribution Security System (EDDS) network. Derived from DSCSA language, the key driver of this functional design is the requirement that all users of the DSCSA EDDS network be "authenticated" or identity-proofed, "authorized,"[1] and specifically, be credentialed.[2] This chapter presents the digital representation of the credentialing process using OCI-specified digital credentials[3] built on W3C standard Verifiable Credentials.

It is important to note that the requirements and recommendations of this Chapter were developed with the perspective of, and apply to, PI Verification and TI Tracing, which may necessitate electronic interaction between trading partners that do not have a direct business relationship. **The credentialing described in this Chapter does not apply to the exchange of TI**, which is definitionally between trading partners with a direct business relationship. While individual trading partners may find business value in extending these credentialing processes to their TI exchange processes and may pursue that as a matter of business practice, PDG does not apply digital credentialing to the TI exchange process, and the requirements and recommendations of this chapter were not designed to address all the considerations that may apply to TI exchange.

Digital Credentials and Manual Processes

In an interoperable environment, it is important that trading partners have a shared understanding of the minimum threshold that must be met by a trading partner to be considered authorized and have its identity authenticated. Chapter 1 defines that minimum threshold. For example, Req-Cred-001 and Req-Cred-010 define the confirmations that are needed to determine whether a manufacturer is "authorized" and Req-Cred-014 defines the confirmations that are needed to authenticate the identity of that manufacturer. Credentials are the way in which an organization demonstrates those thresholds have been met. For the purposes of this document and for the PDG-defined EDDS network (the electronic network), "digital credentials" refers to W3C Verifiable Credentials[4] as applied to the PDG-defined EDDS network by the OCI[5] Open Specifications. As further described in this Chapter, W3C Verifiable Credentials represent an effective and efficient method of credentialing in electronic interactions.

While digital credentials represent an efficient approach to credentialing, PDG also recognizes the practical reality that their adoption will likely be gradual, particularly given competing demands for November 27, 2023 compliance and the learning and maturation processes that will occur after that date. Therefore, PDG recognizes that trading partners may use alternate processes, including company-specific non-automated processes, to demonstrate the threshold assurances of authorized status and identity in Chapter 1 have been met. PDG is optimistic that trading partners will recognize the efficiency of digital credentials during

[1] See Chapter 1 for the definition of "Authorized."
[2] See Chapter 1 for the definition of "Credential" and "Credentialed."
[3] https://www.oc-i.org/resources-portfolio/oci-interop-v2-0-0
[4] https://w3c.github.io/vc-data-model/
[5] The Open Credentialing Initiative publishes open-source specifications and programs for W3C credential issuance and use.

the early period of compliance and migrate toward their use, but the accommodation of manual processes is important to ensure the PDG-defined EDDS network is inclusive of a critical mass of the industry.

Entity Types

PDG has identified three types of organizational identities that will need to access the PDG-defined EDDS network: Authorized Trading Partners (ATP), Authorized Trading Partner Equivalents (ATP-Equivalent), and DSCSA Authorities.

This Chapter represents the functional design and requirements for trading partners, authorities, and supporting solutions that adopt and implement digital credentials for authentication (corporate digital identity) and authorized status (corporate ATP, ATP-Equivalent, or DSCSA Authority status) using W3C[6] standard Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs) as applied to the PDG-defined EDDS network via OCI specifications. This Chapter focuses on the digital credential lifecycle (acquire and maintain digital identity and ATP credentials) used to digitally authenticate and authorize trading partners and authorities in PI Verification and TI Tracing interactions.

PDG evaluated technical options for digital credentialing, considering aspects such as the following:

- Technical trust mechanism (how the technology works);
- Solutions compliance programs;
- Security (cryptography, resistance to tampering and misuse);
- Resilience (from Issuer, Trade Partner private key compromise);
- Confidentiality (Credential Issuer does not participate in credential using interactions and cannot gain business intelligence of their use);
- Choice (no vendor lock-in); and
- Interoperability (with existing PI Verification applications and developing TI Tracing applications).

PDG recognizes and incorporates by reference the Open Credentialing Initiative's set of open-source specifications, which apply W3C standard Verifiable Credentials and Decentralized Identifiers (DIDs) to the PI Verification and TI Tracing functions of the PDG-defined EDDS network. PDG:

- Recognizes W3C DID and Verifiable Credential Standards.
- Recognizes the OCI open specifications and conformance programs.
- Will consider additional approaches as they mature and, if determined to be electronically interoperable, will recognize and incorporate those approaches by reference.

[6] The World Wide Web Consortium (W3C) is the main international standards organization for the World Wide Web.

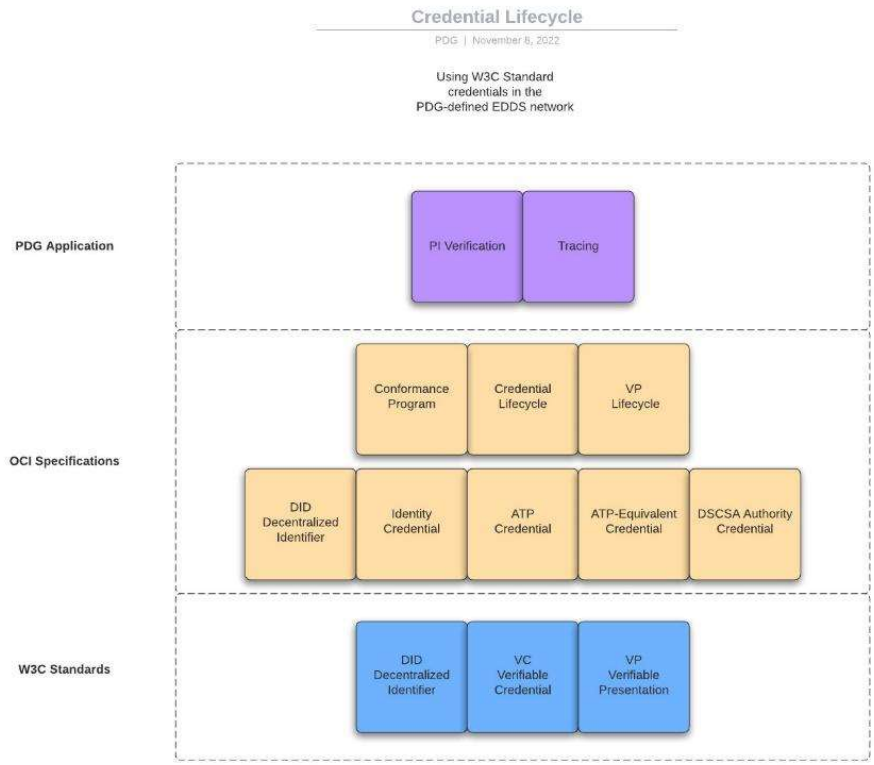

Figure 1- Relationship of PDG Requirements, OCI Specifications, W3C Standards for verifiable credentials.

Purpose of the Document

This Functional Design provides detailed information on *how* verifiable credentials are acquired and maintained by ATPs, ATP-Equivalents, and DSCSA Authority users of the PDG-defined EDDS network. Usage of credentials in the PDG-defined EDDS network PI Verification and TI Tracing digital interactions are addressed in Chapters 4 and 5, respectively. Included in this section are detailed functional designs addressing the use of digital credentials to support Authentication and Authorization processes and policies, participant choreographies, system inputs and outputs, and process flows.

Terminology

Term/Acronym	Definition	Notes
Authentication	The act (process) of proving an assertion, such as the identity of a computer system user.	Wikipedia[7]
Authorization	The function (process) of specifying access rights/privileges to resources, which is related to general information security and computer security, and to access control in particular.	Wikipedia[8]
Authorized	A status whereby: (A) in the case of a manufacturer or repackager having a valid registration in accordance with section 510; (B) in the case of a wholesale distributor, having a valid license under State law or section 583, in accordance with section 582(a)(6), and complying with the licensure reporting requirements under section 503(e), as amended by the Drug Supply Chain Security Act; (C) in the case of a third-party logistics provider, having a valid license under State law or section 584(a)(1), in accordance with section 582(a)(7), and complying with the licensure reporting requirements under section 584(b); and (D) in the case of a dispenser, having a valid license under State law.	From Chapter 1 Glossary
Credential	A tool by which, each organization, as an authorized trading partner, can demonstrate that it meets a set of additional requirements as defined by PDG to ensure they are a valid trading partner who is both uniquely identified and authorized, as required by the DSCSA Functional definition addition: Credential, Digital Credential is represented in this chapter as a W3C Verifiable Credential as applied to PI Verification and TI Tracing by the OCI specifications.	From Chapter 1 Glossary AKA: Digital Credential
Credentialed	For a trading partner, having demonstrated both authorized status and identity according to PDG-defined credentialing process	From Chapter 1 Glossary
Decentralized Identifier (DID)[9]	A type of globally unique identifier that enables an entity to be identified in a manner that is verifiable, persistent (as long as the DID controller desires), and does not require the use of a centralized registry, identity provider or certificate authority.[10] DIDs enable a new model of decentralized digital identity that is often referred to as self-	

[7] https://en.wikipedia.org/wiki/Authentication.
[8] https://en.wikipedia.org/wiki/Authorization.
[9] *"Decentralized Identifiers (DIDs) v1.0"*. *World Wide Web Consortium*.
[10] *"Decentralized Identifiers (DIDs) v1.0"*. *World Wide Web Consortium*.

	sovereign identity or decentralized identity.[2] They are an important component of decentralized web applications.	
DID Document	A decentralized identifier resolves (points) to a **DID document**, a set of data describing the DID subject, including mechanisms, such as cryptographic public keys, that the DID subject or a DID delegate can use to authenticate itself and prove its association with the DID[5].	
DID Resolution	The process that takes as its input a DID and a set of resolution options and returns a DID document in a conforming representation plus additional metadata.	
DID Controller	An entity that has the capability to make changes to a DID document. Note, for the purpose here, a DID controller is typically the DID subject.	
DID Subject	The entity identified by a DID and described by a DID document. Anything can be a DID subject: person, group, organization, physical thing, digital thing, logical thing, etc.[5] For the purpose of the PDG-defined EDDS network, the DID Subject is the ATP, ATP-Equivalent or DSCSA Authority who owns or controls the verifiable credential.	
Digital Credential	For the purposes of the PDG-defined EDDS network, a digital credential is defined as an OCI-specified representation of a W3C Standard Verifiable Credential meeting the business requirements associated with credentialing within the electronic network.	
Verifiable Credential	A standard data model and representation format for cryptographically verifiable credentials as defined by the W3C Verifiable Credentials specification [VC-DATA-MODEL] and specified by OCI for use in DSCSA processes of PI Verification and TI Trace.	
Verifiable Presentation	Expresses data from one or more Verifiable Credentials as defined by the W3C Verifiable Credentials specification [VC-DATA-MODEL] and specified by OCI for use in DSCSA processes of PI Verification and TI Trace. The Verifiable Presentation is packaged in such a way that the authorship of the data is cryptographically verifiable.	
Credential Revocation	Credentials are revoked by the Issuer of the credential through a revocation list due to a status change of the ATP, ATP-Equivalent, or DSCSA Authority. The revocation method is documented in the credential itself.	
Digital Wallet	Software solution utilized to manage Decentralized Identifiers and to acquire, store, present, and verify Verifiable Credentials.	

Verification Methods	The Verification Method property of the Verifiable Credential specifies; for example, the public key that can be used to verify the digital signature.	

Standards, Specifications, and Guidelines

The following standards, specifications, and guidelines are pivotal to the proper implementation of a digital credentialing ecosystem needed to support digital credential issuance and revocation, as well as digital identity and key management. Although open to technology advances in the future, PDG recognizes and incorporates the W3C standards for decentralized identification and verifiable credentials and the Open Credentialing Initiative (OCI) architecture for managing those elements in relationship to PDG-defined EDDS network digital interactions of PI Verification and TI Tracing.

Table 1 – digital credentialing Reference Documents

Reference Document	Version	Publisher	Notes
Open Credentialing Initiative - Getting Started		Open Credentialing Initiative	Resources for VRS, TI Tracing, Wallet and Issuer solutions
OCI GitHub		Open Credentialing Initiative	OCI Governance and Specification Repository
OCI Interoperability Profile	2.0.0	Open Credentialing Initiative	Maintains interoperability between OCI specifications
Credential Issuer Conformance Criteria	2.0.0	Open Credentialing Initiative	
Digital Wallet Conformance Criteria	3.0.0	Open Credentialing Initiative	
Credential Schemas	1.0.0	Open Credentialing Initiative	
Digital Wallet Provider OpenAPI Specification	2.0.0	Open Credentialing Initiative	
Integration with VRS Providers	3.0.0	Open Credentialing Initiative	
OCI Trusted Issuer Registry	1.0.0	Open Credentialing Initiative	
OCI Conformance Program	1.0.0	Open Credentialing Initiative	
VRS Provider Conformance Criteria	Draft	Open Credentialing Initiative	

OCI mapping to PDG *Blueprint*	Pub 2022-02-01	Open Credentialing Initiative	
Digital Identity Guidelines: Enrollment and Identity Proofing (SP 800-63A)	Pub 2020-03-202	NIST	
Decentralized Identifiers (DIDs)	1.0	W3C	
Verifiable Credentials Data Model	2.0	W3C	

Use of Open Specifications for Credentialing

The OCI architecture is based on decentralized public key infrastructure (PKI) technology and identity anchoring mechanisms to set up a digital identity for the trading partners and credential issuers involved.

Both the abstract concepts and the concrete implementations of verifiable credentials (VCs) using decentralized identifiers (DIDs) have been gaining momentum and acceptance. The primary forums of activity in developing interoperable open standards for these are the World Wide Web Consortium (W3C) and the Decentralized Identity Foundation (DIF). Working groups at the W3C authored and maintain the W3C Verifiable Credential Data Model 1.0 specification. The W3C Verifiable Credentials Data Model is a W3C recommendation (the most mature stage of the W3C standards process). Verifiable credentials (VCs) are issued against identifiers that may be associated with cryptographic operations, be they DIDs, self-certifying identifiers, or legacy identities backed with traditional PKI.

The most important class of identifiers for verifiable credentials, however, is a Decentralized Identifier (DID). The W3C Decentralized Identifiers (DIDs) specification is a W3C recommendation.

To fulfill the DSCSA requirements, the OCI architecture uses the following components:

- W3C Decentralized Identifiers (DIDs),
- W3C Verifiable Credentials (VCs), and
- Digital Wallets.

The Trading Partners applying OCI's architecture require a digital wallet. The digital wallet is a software component that manages the DIDs and VCs that are required for authentication and authorization. OCI-conformant Digital Wallets are required to expose an interface that enables DSCSA solution providers to use a Trading Partner's Credentials to facilitate authentication and authorization on their behalf. To ensure interoperability among digital wallets, the OCI published conformance criteria for Digital Wallet providers.

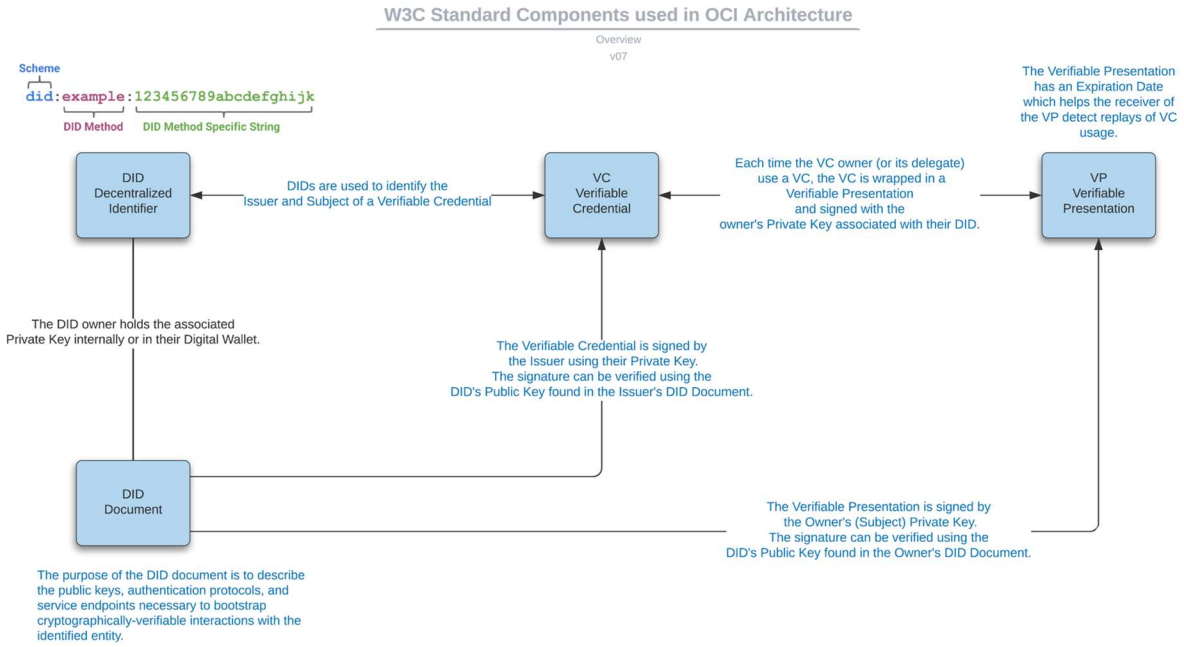

Figure 2a – W3C Standards used in OCI Specifications.[11]

Authentication, Authorization, and Credentialing Overview

Authentication and Authorization in a Decentralized, Digital Network

The PDG-defined EDDS network is an electronic, highly distributed network of systems supporting DSCSA requirements for trading partners. As such, participants in this electronic network need to be able to Authenticate and Authorize each other in DSCSA electronic interactions. For TI/TS Exchange, current supplier/buyer onboarding processes and information are used in the Authentication and Authorization steps. Given the dynamic nature of PI Verification and interoperable TI Tracing interactions where participants in those electronic interactions may not have an existing relationship, verifiable information about the parties in these interactions is needed to support Authentication and Authorization decisions and system configurations. *Figure 2b* illustrates the highly distributed nature of the PDG-defined EDDS network and the need for a mechanism supporting Authentication and Authorization across the network and between networked solutions.

[11] OCI: https://www.oc-i.org/resources-portfolio/oci-technical.

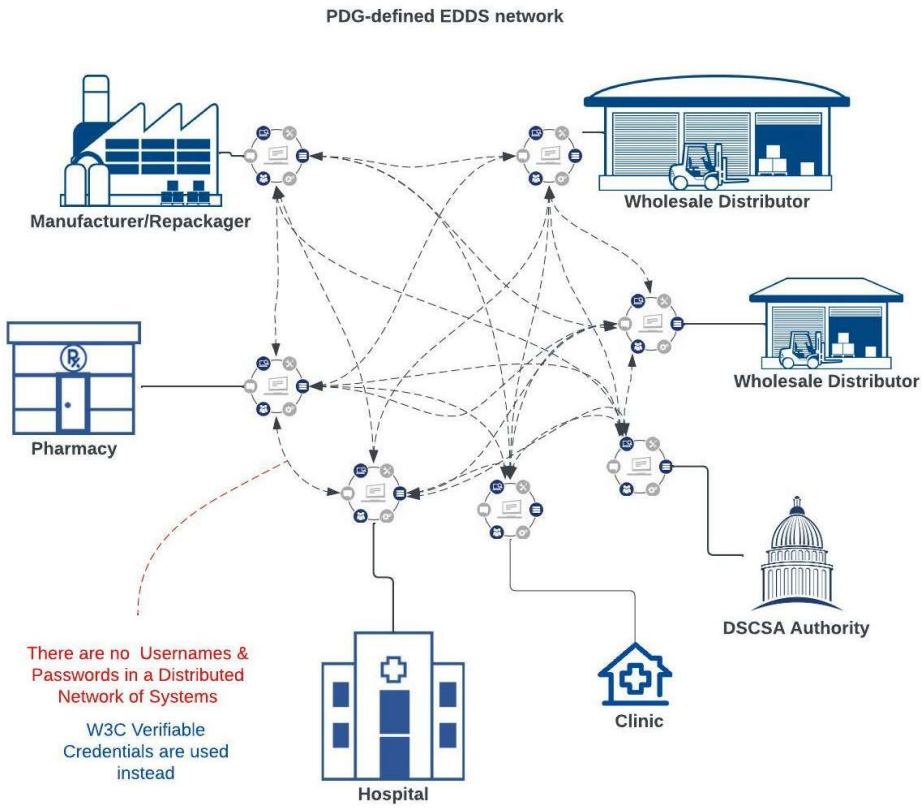

Figure 2b: An illustration of the highly distributed nature of the PDG-defined EDDS network.

The following table provides insights into the value of using VCs in the PDG-defined EDDS network for PI Verification and TI Tracing electronic interactions.

Function	Verifiable Credential Method	Non-Credential Method
Authentication: Verify the counterparty in the electronic interaction (PI Verification or TI Tracing) is who they say they are.	**Verifiable Credential Issuance:** By performing thorough and auditable due diligence, a Credential Issuer assures confidence in a Trading Partner's digital identity prior to the issuance of an ATP, ATP-Equivalent, or DSCSA Authority Credential. The Identity Credential becomes the Root of Trust upon which an ATP, ATP-Equivalent or DSCSA Authority Credential can be issued." The party receiving such verifiable credential can trust that the holding party has been identity-verified.	Contact party using PI Verification or TI Tracing Contact Information. Use internal policies to guide Authentication.
Authentication: Verify the counterparty in the electronic interaction (PI Verification or TI Tracing) is who they say they are.	**Verifiable Credential Usage:** Digital Wallet uses cryptographic processes to verify the Issuer's and Party's signatures on the presented digital credential. The Digital Wallet checks if the signatures match the public keys available in the openly accessible DID Document of the Issuer or Party. Specific Digital Wallet checks: ● Trusted Issuer List, ● Issuer's digital signature in digital credential, and ● Identifying information in the credential.	While in contact with the Party using PI Verification or TI Tracing electronic messages, verify that they sent the electronic request or response.

Authorization: Verify that the party has a current ATP, ATP-Equivalent, or DSCSA Authority status.	Digital Wallet verifies that the ATP, ATP-Equivalent, or DSCSA Authority digital credential that is attached to a PI Verification or TI Tracing Message is not expired.	Look up or access your up-to-date records of the party's Federal registration (if they are a manufacturer or repackager), or State license. For State-licensed parties, the counterparty may need to be contacted for a State license number and the associated State in order to verify the license against that State's published records.
Authorization: Verify that the electronic request or response is allowed for this party. ● The same process applies to both verifiable credential and non-credential method.	**Application of Business Rules:** Chapters 1, 4 (PI Verification), and 5 (TI Tracing) provide constraints on interactions permissible for PI Verifications and TI Trace requests/responses. The PI Verification or TI Trace solution will encode and enforce these constraints.	**Application of Business Rules:** Chapters 1, and 4 (PI Verification), and 5 (TI Tracing) provide constraints on interactions permissible for PI Verifications and TI Trace requests/responses. The PI Verification or TI Trace solution will encode and enforce these constraints.

Security: Verify that Authentication and Authorization proofs have not been tampered with or provided by an unauthorized party (request or response replay, unauthorized use of proof, etc.).	1. The presented credential is cryptographically checked by Digital Wallet to ensure it has not been tampered with. 2. PI Verification and TI Trace solutions use the Digital Wallet to verify the Party's digital signature in the Verifiable Credential Presentation (VP) to ensure the Party approved usage of their credential for this electronic interaction (PI Verification or TI trace). 3. PI Verification and TI Trace solutions use the Digital Wallet to check the credential presentation timeout to ensure the credential isn't reused by an unauthorized party.	Follow internal policies and processes for checking proofs provided by parties in the interaction.

Before diving into the technical aspects of credential life cycles, it is important to understand the statutory, regulatory, industry-agreed, and individual organization requirements and policies on systematic authentication and authorization as it relates to the PDG-defined EDDS network.

Figure 3 illustrates how requirements and policies of the DSCSA statute, FDA regulations, FDA guidances, industry consensus, and individual organization internal policies affect the technical architecture of the PDG-defined EDDS network and specifically the use of digital verifiable credentials within this electronic network.

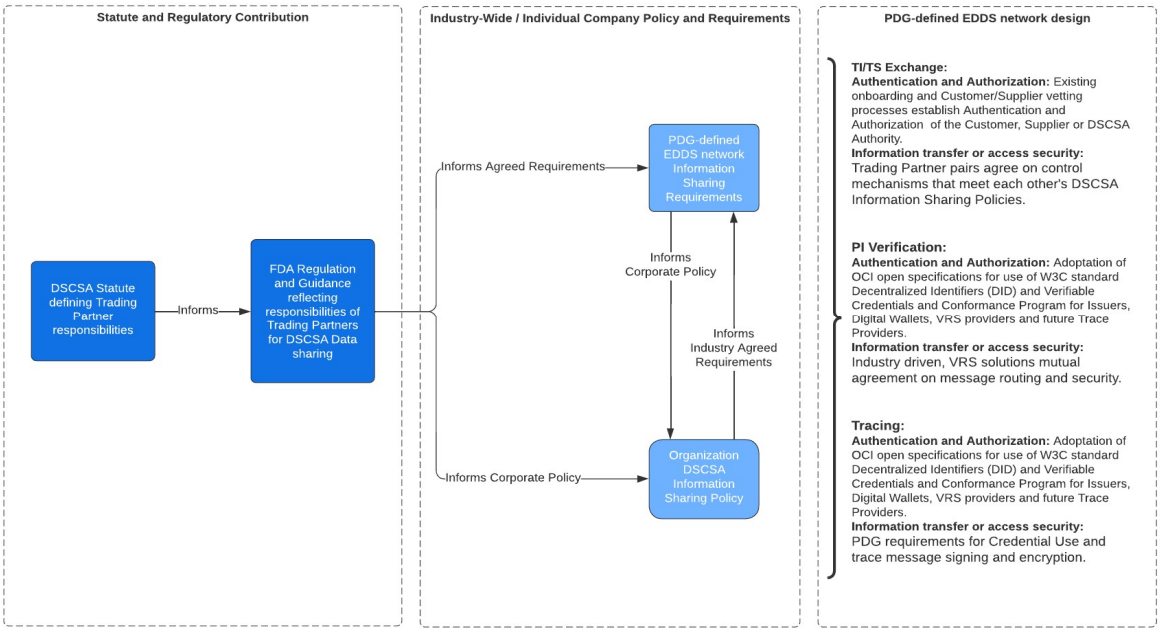

Figure 3– Authentication and Authorization are driven by statute, regulatory and industry requirements and policies.

Chapter 1 provides the statutory and PDG definitions of:

- Authorized,
- Credential,
- Credentialed,
- Licensed,
- Interoperability, and
- System.

These definitions inform the Functional Design for the use of digital credentials within the digital PDG-defined EDDS network providing the information and process assurance (or trust) needed for authentication and authorization processes.

Authentication

In an Authentication process, the identity of the user is checked in order to provide access to the system. For the purposes of electronic interactions in the PDG-defined EDDS network, Authentication means the process of verifying the identity of the user entity in electronic interaction.

Authorization

In an Authorization process, the user's authority to access a resource is checked. Authorization follows Authentication. For the purposes of electronic interactions in the PDG-defined EDDS network, Authorization means the process of verifying the ATP, ATP-Equivalent, or DSCSA Authority status.

Authentication and Authorization for DSCSA electronic interactions.

Three main electronic interactions have been identified for the PDG-defined EDDS network: TI/TS Exchange, PI Verification, and TI Tracing. The following table illustrates how PDG-defined EDDS network participant Authentication and Authorization processes are supported for network interactions.

Interaction	Authentication Support	Authorization Support	Verifiable Credential Verification Checks
TI/TS Exchange	Existing processes for onboarding trading partners	Existing processes for checking trading partner FDA registration(s)[12] or State license(s)	N/A
PI Verification	Verified identity of the counterparty	Verified ATP, ATP-Equivalent or DSCSA Authority Credential	1. Presentation of Credential hasn't timed out 2. Trading Partner's digital signature on Credential Presentation verifies 3. Issuer's digital signature on Credential verifies 4. The credential Issuance date is not greater than Today's date 5. The credential is not expired 6. The credential has not been revoked 7. The credential has not been tampered with
TI Tracing	Verified identity of the counterparty	Verified ATP, ATP-Equivalent or DSCSA Authority Credential	1. Presentation of Credential hasn't timed out 2. Trading Partner's digital signature on Credential Presentation verifies 3. Issuer's digital signature on Credential verifies 4. The credential Issuance date is not greater than Today's date 5. The credential is not expired 6. The credential has not been revoked 7. The credential has not been tampered with

[12] https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/are-you-ready-drug-supply-chain-security-act.

Meeting the PDG Credentialing Requirements

The OCI mapping to PDG *Blueprint* document provides details on how the OCI specifications support business and compliance requirements of the PDG *Blueprint*. Chapters 4 (PI Verification) and 5 (TI Tracing) include functional requirements and illustrations that address how the digital credentials defined here are implemented within those functional areas to meet industry expectations.

OCI specifications apply W3C Verifiable credentials to the PDG-defined EDDS network PI Verification and TI Tracing electronic interactions, addressing the following priorities outlined by the DSCSA community:

Interoperability. By allowing solutions to adopt the same schemas, APIs, etc., OCI open standards and specifications allow competing solutions to interoperate within the PDG-defined EDDS network.

Assurance. Trust for others' credentials is built on open published standards and open specifications for identity assurance, authorization, and security.

Security. The standards and open specifications include the use of signatures and other cryptographic features appropriate for a decentralized ecosystem such as the PDG-defined EDDS network.

Confidentiality. OCI specifies a separation of duties – the issuer is not involved with transactions, and wallets are limited in access to transaction data. This mitigates unauthorized business intelligence gathering and correlation.

Choice. Thanks to interoperability between solutions in the PDG-defined EDDS network, service users are not locked into any single vendor.

Convenience. Complete or partial process automation alleviates the necessity for manual (and potentially repetitive) authentication and authorization processes.

Economical. Electronic credentialing allows the pharmaceutical supply chain to avoid the costs of manual authentication and authorization processes.

Credentialing Ecosystem

This document addresses the technical details of using digital credentials to inform authentication and authorization decisions in PI Verification and TI Tracing interactions. Trading partner systems manage the checks and usage of credentials in the PDG-defined EDDS network (internal or contracted solutions).

From a trading partner perspective, acquiring, maintaining, and using credentials is seamless and often occurs behind the scenes, with minimal differences compared to other solution onboarding processes.

The Credentials

A credential is a set of one or more claims made by an issuer about a holder of a credential. Within the PDG-defined EDDS network, there are three defined types of organizations that should be credentialed:

1. Authorized Trading Partner (ATP): Trading partners who hold an FDA Registration or State license;
2. Authorized Trading Partner Equivalent (ATP-Equivalent): Trading partners who do not hold (or may not be required to hold) an FDA registration or State license. ATP-Equivalents are included in the PDG ATP-Equivalent organizations list;[13] and
3. DSCSA Authorities: Authorities included in the PDG DSCSA Authority list.[14]

Based on the enterprise identity verification the credential issuer will issue an **identity credential to the holder DID. The Identity Credential** is used as the root of trust for the EDDS network. Based on the identity credential, the Credential Issuer can issue digital credentials to authenticate users on the PDG-defined EDDS network as authorized parties:

1. DSCSA ATP Credential,
2. DSCSA ATP-Equivalent Credential, and
3. DSCSA Authority Credential.

These credentials follow the format and structure set in the OCI specifications[15] and are managed by Issuers and acquiring organizations using Digital Wallet solutions. *Figure 4* illustrates the interactions between an Issuer and Trading Partner or DSCSA Authority for acquiring these credentials.

Identity Credential
An organizational identity credential ensures the organization has been identity proofed by independently validating the applicant's claim to represent a particular organization.

DSCSA ATP Credential
The ATP credential is used by trading partners who do meet the explicit requirements of "Authorized" in the statute. That is, they are organizations that are required to hold an FDA registration or State license.

DSCSA ATP-Equivalent Credential
The ATP-Equivalent credential is used in place of an ATP Credential by trading partners who are not required to hold an FDA registration or State license but are engaged in DSCSA transfer of ownership transactions.

DSCSA Authority Credential
The DSCSA Authority Credential is used in place of the ATP Credential by DSCSA Authorities within the PDG-defined EDDS network to support authentication and authorization processes of trading partners for PI Verification and interoperable TI Tracing interactions.

The Verifiable Credentialing Process
Chapter 1 defines the requirements for an Identity Credential and ATP Credential. An entity's PI Verification or TI Tracing solution will typically facilitate the entity's acquisition of these credentials. Much like the process of notarizing corporate documents, the trading partner will interact with an issuer of the Identity and ATP (or ATP-Equivalent or DSCSA Authority) credential.

[13] see Recommendations section.
[14] see Recommendations section.
[15] https://www.oc-i.org/resources-portfolio/oci-interop-v2-0-0.

Enterprise Identity Verification

By performing thorough and auditable due diligence, a Credential Issuer promotes confidence in a Trading Partner's digital identity prior to the issuance of an ATP credential.

Prior to credential issuance, a trading partner's enterprise identifier (DID) needs to be verified through an identity verification process. Enterprise identity verification is completed by the Credential Issuer according to OCI-defined conformance criteria for Credential Issuers. Upon successful verification, the Credential Issuer will release an identity credential that is used as the Root of Trust within the ecosystem.

Authorization Status Verification

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

Credential Lifecycle Management

An Issuer of an Identity or ATP Credential must also periodically re-verify the identity of the company and its ATP status. They must also maintain a revocation registry accessible by the Digital Wallet that establishes individual entries for credentials that fail due diligence.

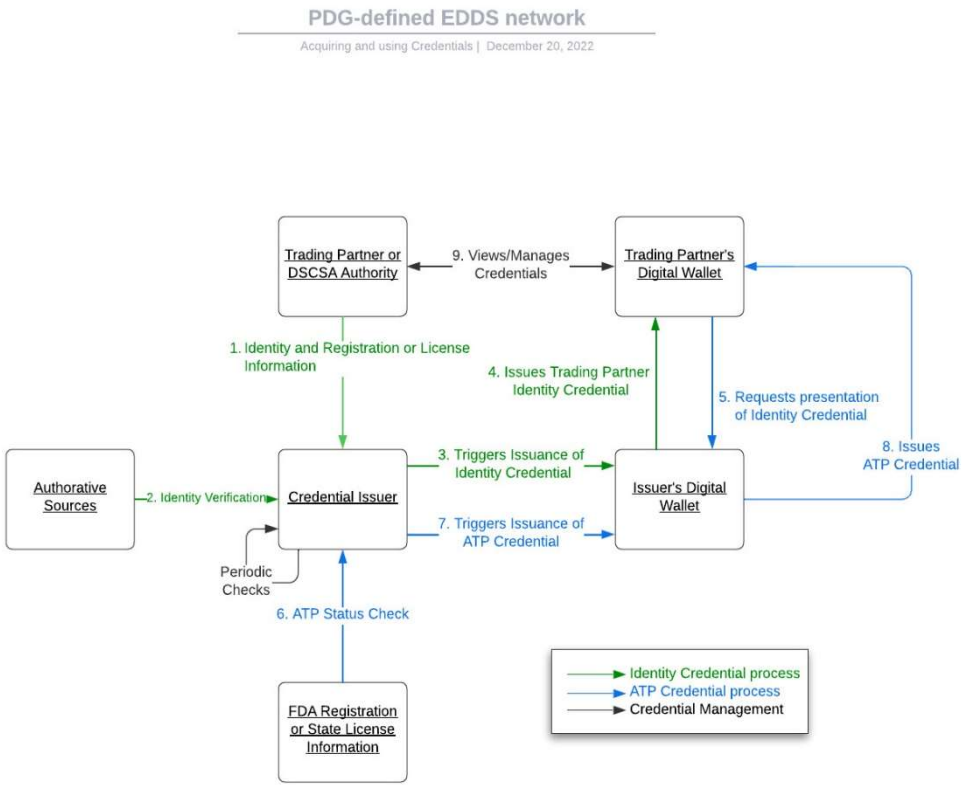

Figure 4 - Acquiring Verifiable Credentials.

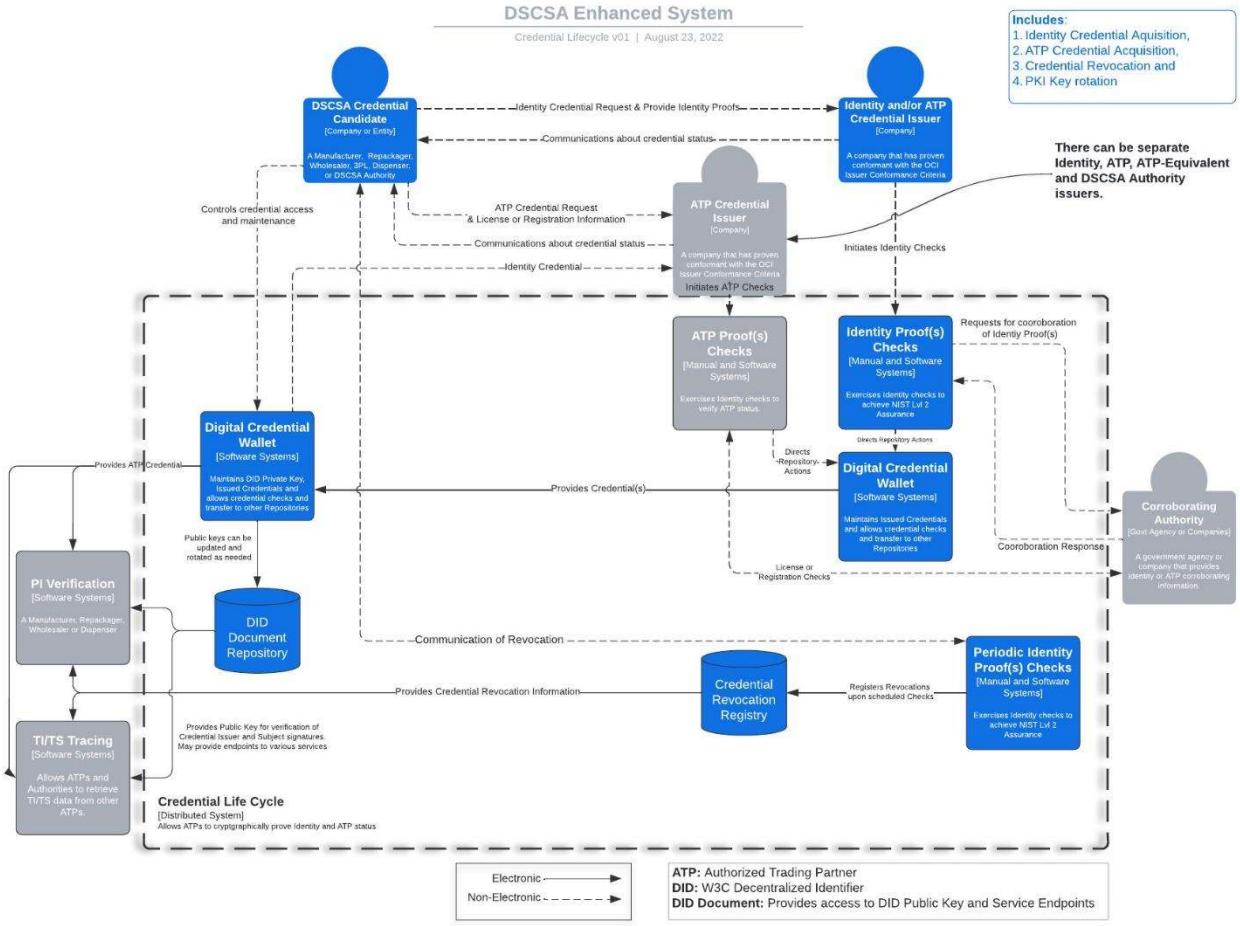

Figure 5 – verifiable credential Lifecycle Management.

Credential Architecture Illustration

Figure 6 illustrates how a W3C standard Verifiable Credential (OCI DSCSA ATP Credential visualized) is configured within a Verifiable Presentation and adapted to the existing PI Verification VRS.

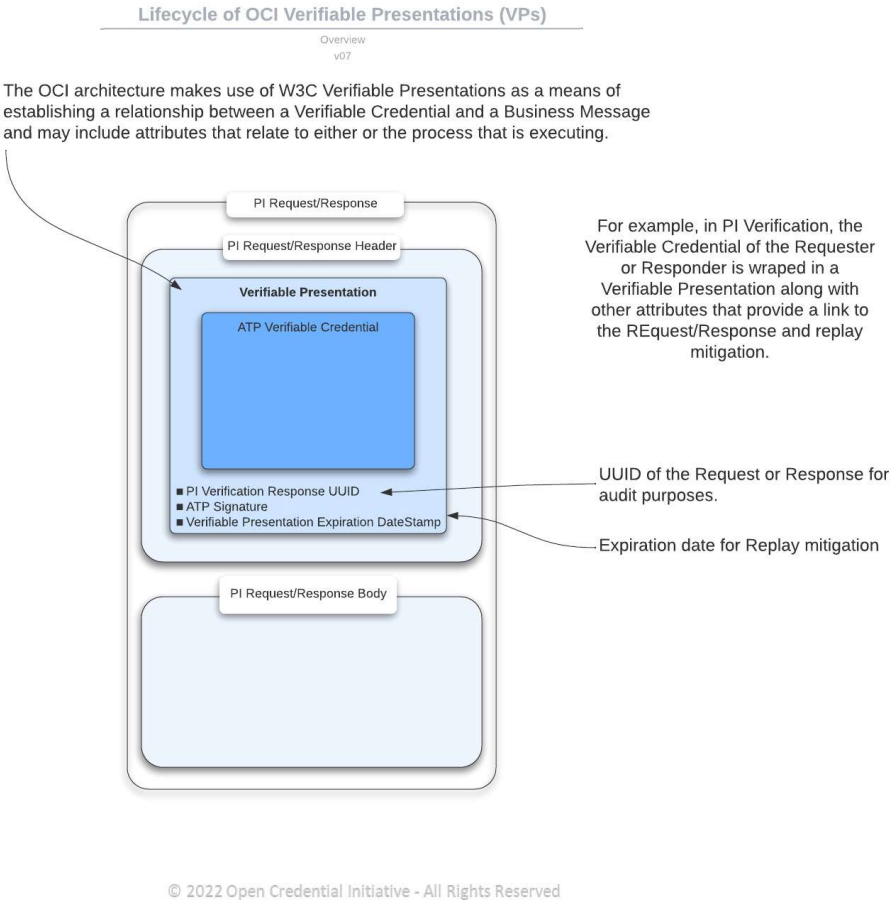

Figure 6 - verifiable credential used in PI Verification Requests and Responses.[16]

[16] OCI Contribution.

Verifiable Credential Lifecycle Illustration

Figure 7 illustrates typical interactions in acquiring and maintaining Verifiable Credentials for use in the PDG-defined EDDS network for PI Verification and TI Trace interactions.

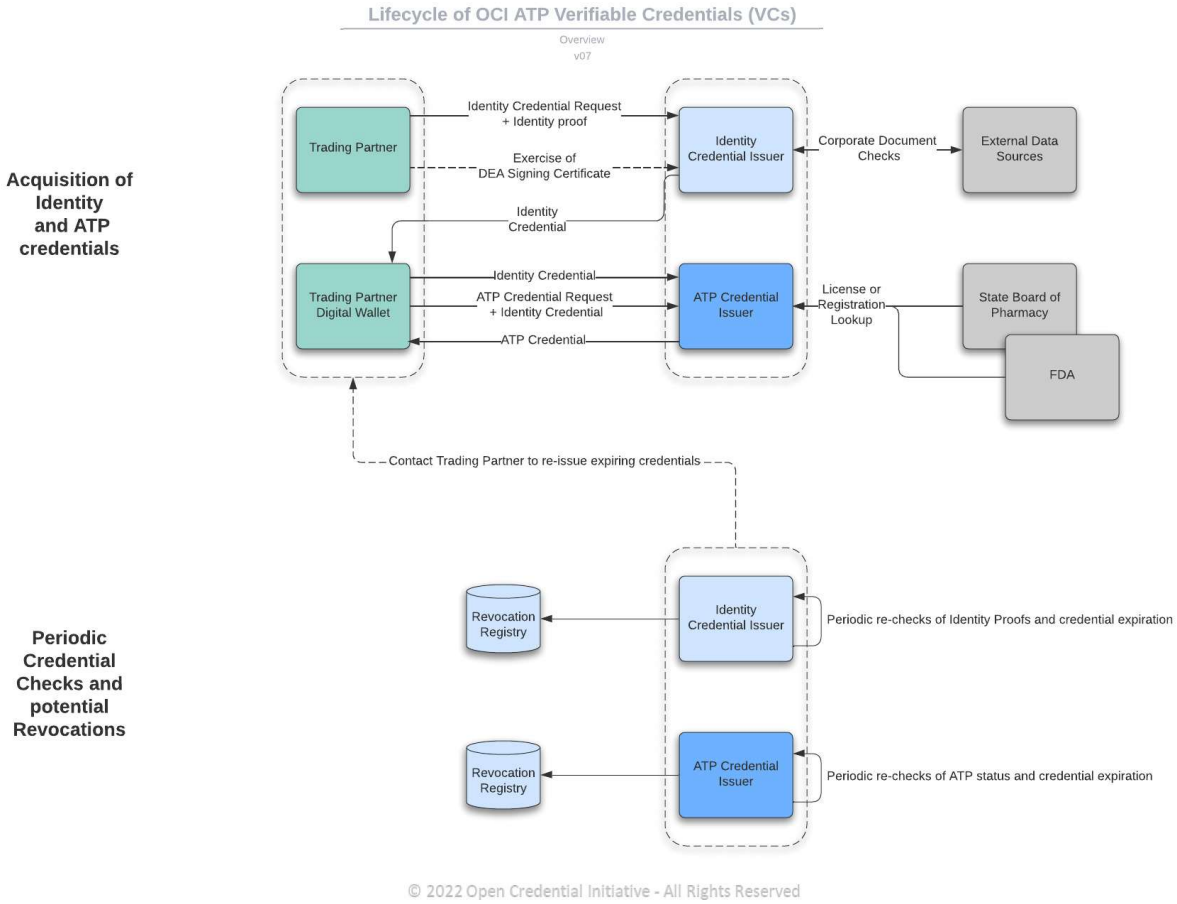

Figure 7 - ATP Credential Lifecycle.[17]

[17] OCI Contribution: *https://www.oc-i.org/resources-portfolio/oci-technical*.

Decentralized Identifier (DID) Lifecycle

W3C Verifiable Credentials rely on the use of W3C standard Decentralized Identifiers (DIDs) and publicly accessible DID Documents to verifiably identify an entity without the use of central registries.

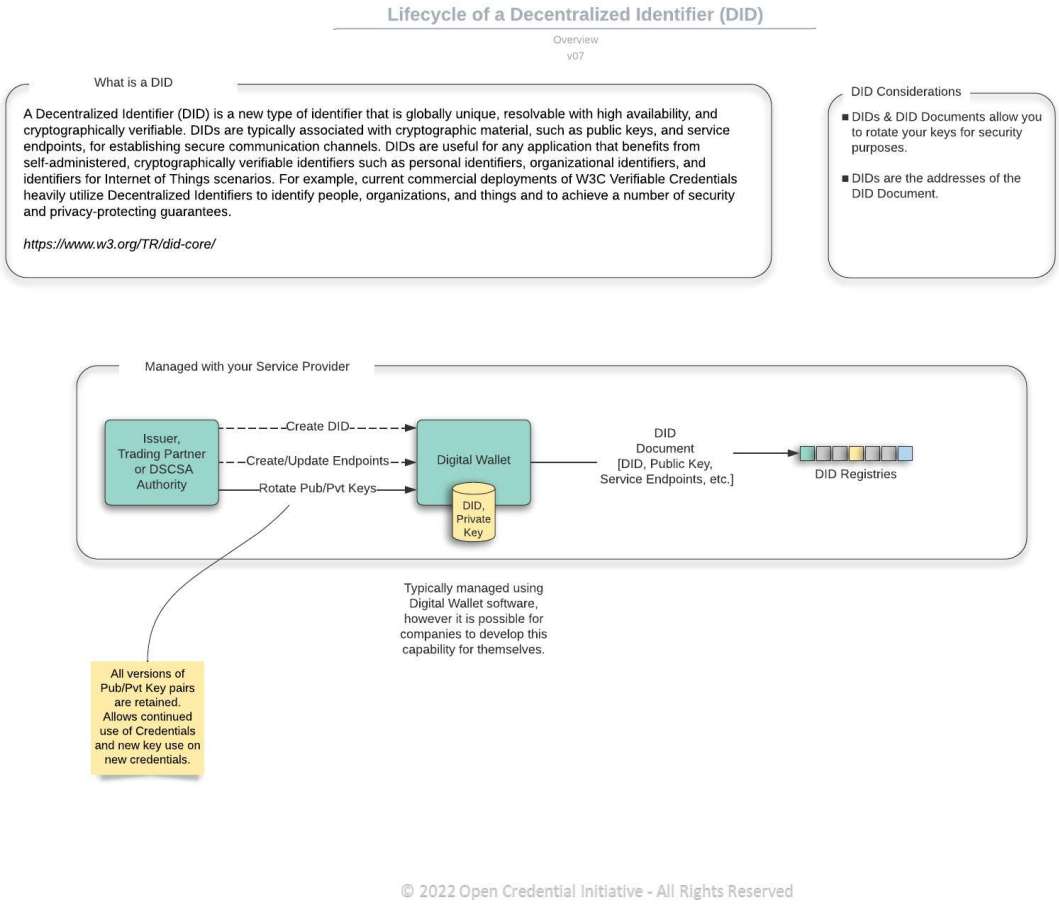

Figure 8 - Decentralized Identifier (DID) Lifecycle illustration.[18]

[18] OCI Contribution.

Digital Credentials in PI Verification and TI Tracing Interactions

For electronic communication as part of Interoperable PI Verification and Interoperable TI Tracing, digital credentials allow for efficient and effective authentication and authorization of counterparties participating in the communication. The nuances of how credentialing architecture and behind-the-scenes processes contribute to the ability of trading partners and their systems to digitally authenticate and authorize each other are illustrated by looking at the architecture from governance, solutions (internal and external), processes, and the credential technology itself:

Governance

- PDG *Blueprint*
- OCI Conformance Program[19]
- PDG/OCI coordination
- GS1 US Lightweight Messaging Standard for PI Verification

Conformance

- Credential Issuers conform to the requirements[20]
- Digital Wallet solutions conform to the requirements[21]
- PI Verification solutions conform to the requirements[22]
- Traceability solutions conform to the requirements[23]

Roles

Credential Issuer

- Initial and ongoing due diligence of identity and ATP authorization
- Has access to OCI conformant Digital Wallet that it uses to issue and verify credentials (ATP & Identity)
- Signs issued Credentials with own Public Key that is accessible for verification in public DID Document
- Monitors issued credentials on a frequent basis
- Revokes issued credentials of entities that fail periodic re-checks

Trading Partner (ATP and ATP-Equivalent) and DSCSA Authority

- Has access to OCI conformant Digital Wallet that it uses to hold, present and verify credentials (ATP & Identity)
- Authorizes PI Verification and TI Tracing service providers to access digital wallet to create a credential presentation and verify credential presentations.
- Digital Wallet signs all credential presentations, verifies inbound credentials, and maintains their public key in a publicly accessible DID Document
- Digital Wallet creates an audit trail of all presented and verified credentials mapped to PI Verification or TI Tracing interactions
- Can audit how their own credentials have been used on their behalf and how third-party credential presentations have been verified in a certain process

[19] OCI Conformance Program.
[20] OCI Credential Issuer Conformance Criteria.
[21] OCI Digital Wallet Conformance Criteria.
[22] Pending OCI VRS Solution Conformance Criteria.
[23] Pending Tracing Solutions verifiable credential Conformance Criteria.

PI Verification and TI Tracing Solution Providers

- Integration with Digital Wallet APIs
- VRS solution has the authorization to use[24] digital wallet APIs
- Attach Trading Partner ATP credential to outbound PI Verification or TI Tracing Messages
- Verify incoming ATP credentials attached to inbound PI Verification or TI Tracing Messages

Components

- GS1 Lightweight Messaging standard
- W3C specified Decentralized Identifiers (DIDs),
- W3C specified Verifiable Credentials (VCs),
- W3C specified Verifiable Presentations (VPs),
- OCI Trusted Issuer List,
- Verifiable Credential Revocation Registry
- OCI specified Digital Wallets

[24] Request generation of a credential presentation and request verification of a credential and its presentation.

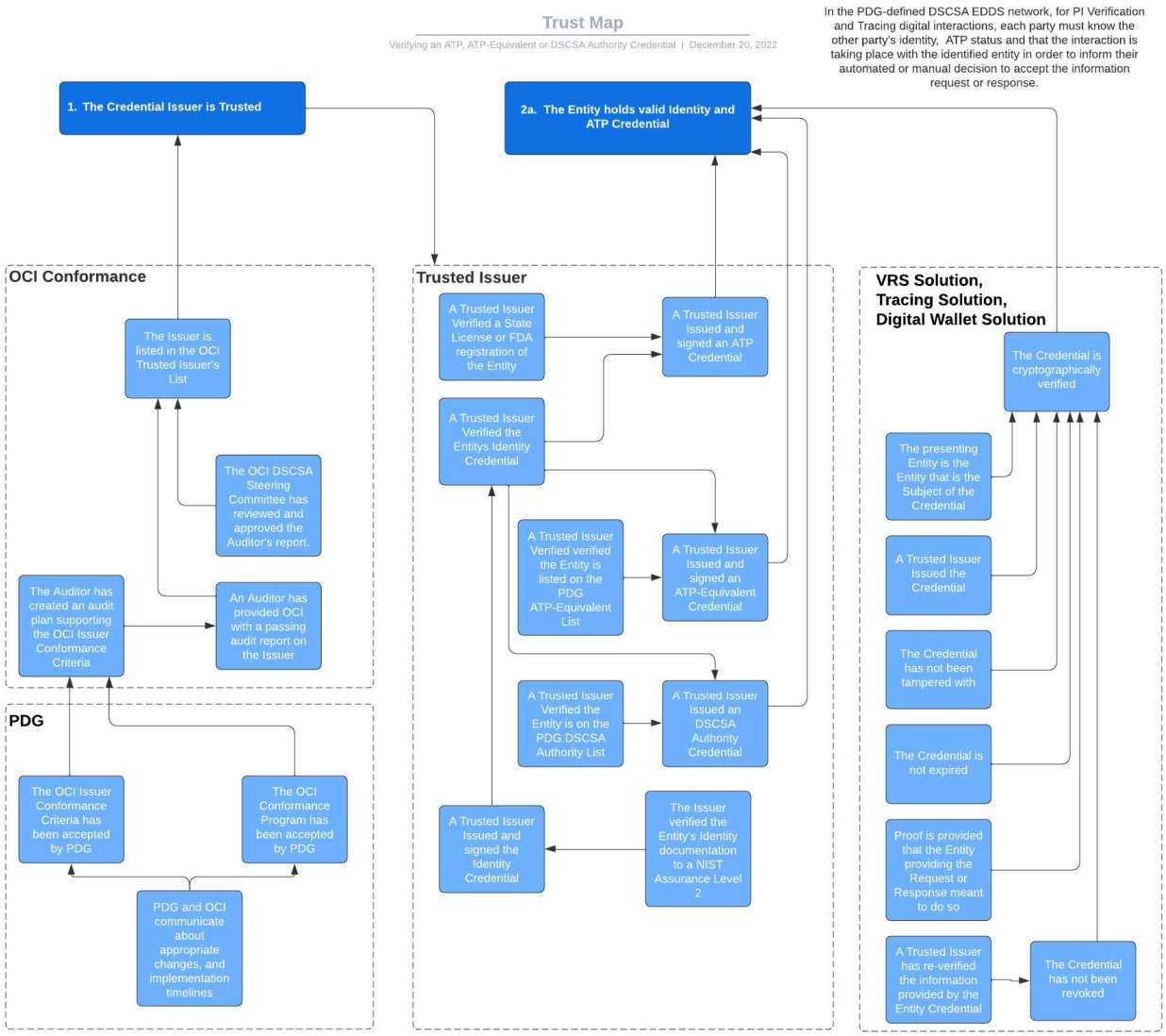

Figure 9 - Trust map for Verifiable Credentials used in the PDG EDDS network.

Verifiable Credentials for PI Verification

Within the PDG-defined EDDS network, PI Verification occurs through the established Verification Router Service (VRS) network or directly between PI Verification systems or services.[25]

The digital credential architecture adopted by PDG is to support an interoperable, electronic, and decentralized ecosystem for both PI Verification[26] and TI Tracing. However, PDG recognizes that individual trading partner pairs may address authentication and authorization outside the PDG-defined DSCSA EDDS network. Two alternatives have been proposed:

KYC/KYS and direct connections: In the same way TI/TS exchange relies on trading partner pairs establishing authentication and authorization through their established KYC/KYS processes and by establishing direct and secure connections between their systems.

Non-Credentialed process: For an entity to respond to a PI Verification or TI Tracing request or to accept a PI Verification or TI Tracing response, they must first ascertain the counterparty's identity and "authorized" status and ensure that the party represented in the interaction initiated the PI Verification or trace. Contact Information provided in PI Verification and TI Tracing messages can aid in initiating the Authentication and Authorization process.

[25] Chapter 4 – PI Verification.
[26] Chapter 4, PI Verification also identifies verification via replicate TI/TS data which makes use of trading partner authentication and authorization between known trading partners along the lines of TI/TS exchange.

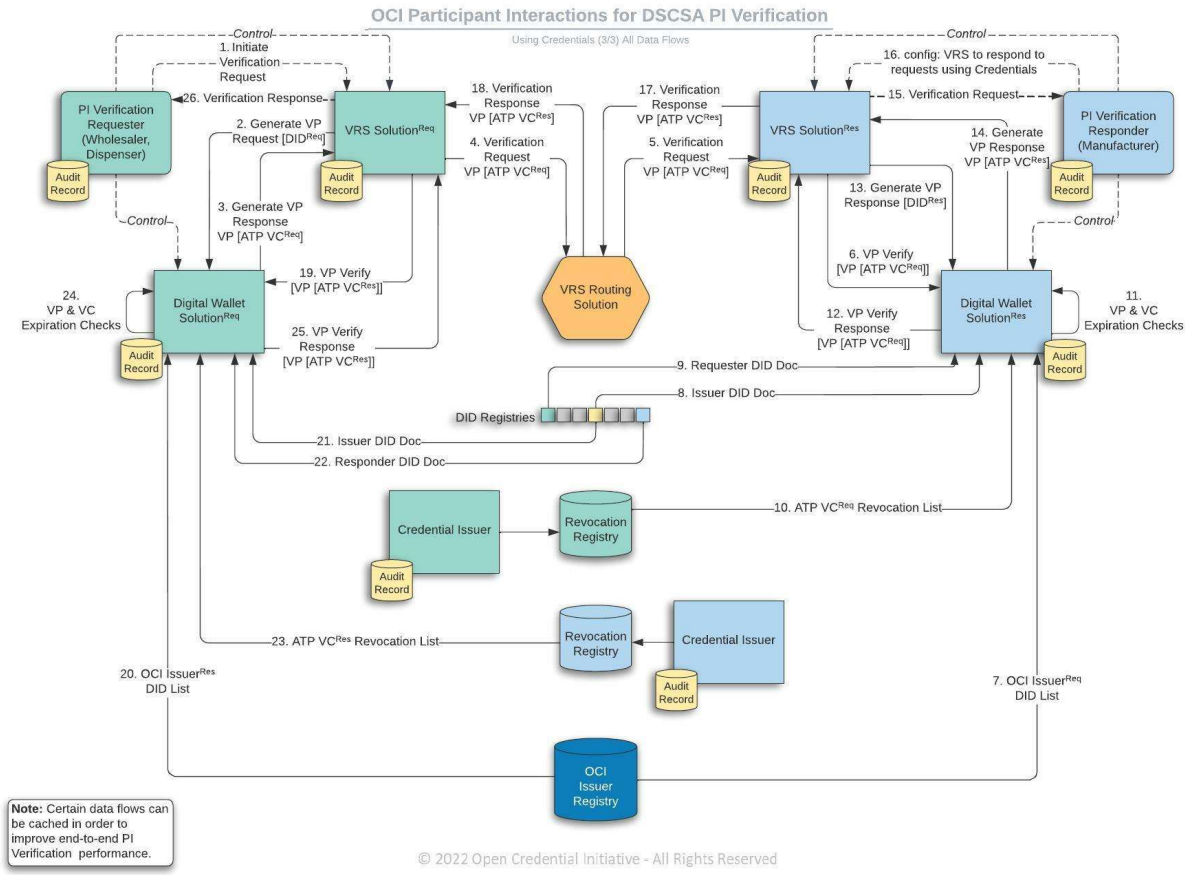

Figure 10 - Illustration of verifiable credential use in PI Verification interactions.[27]

The OCI-conformant digital wallet providers need to furnish the VRS providers with APIs to:

1. **Generate** a Verifiable Presentation of a DSCSA ATP Credential in form of a JSON Web Token (JWT) and
2. **Verify** a Verifiable Presentation of a DSCSA ATP Credential.

The diagrams below depict how digital wallets for credential management are integrated into the existing PI verification systems utilized by VRS providers.

Generate an OCI conformant ATP Credential Presentation

GS1 provides a standardized Lightweight Verification Message format that can be implemented by all VRS providers. The required verifiable credential presentation is added in the form of a JWT to the message header, leaving the message body unchanged.

The VRS calls the Digital Wallet APIs by providing the CorrUUID, DID, and the required credential type. The response from the Digital Wallet is a JWT including the Verifiable Presentation of the DSCSA ATP

[27] OCI Contribution.

Credential. The JWT is attached to the verification request message header. The VRS can do this for any Trading Partner who authorizes them to use their digital wallet that holds credentials.

The PI request process is depicted in the figure below:

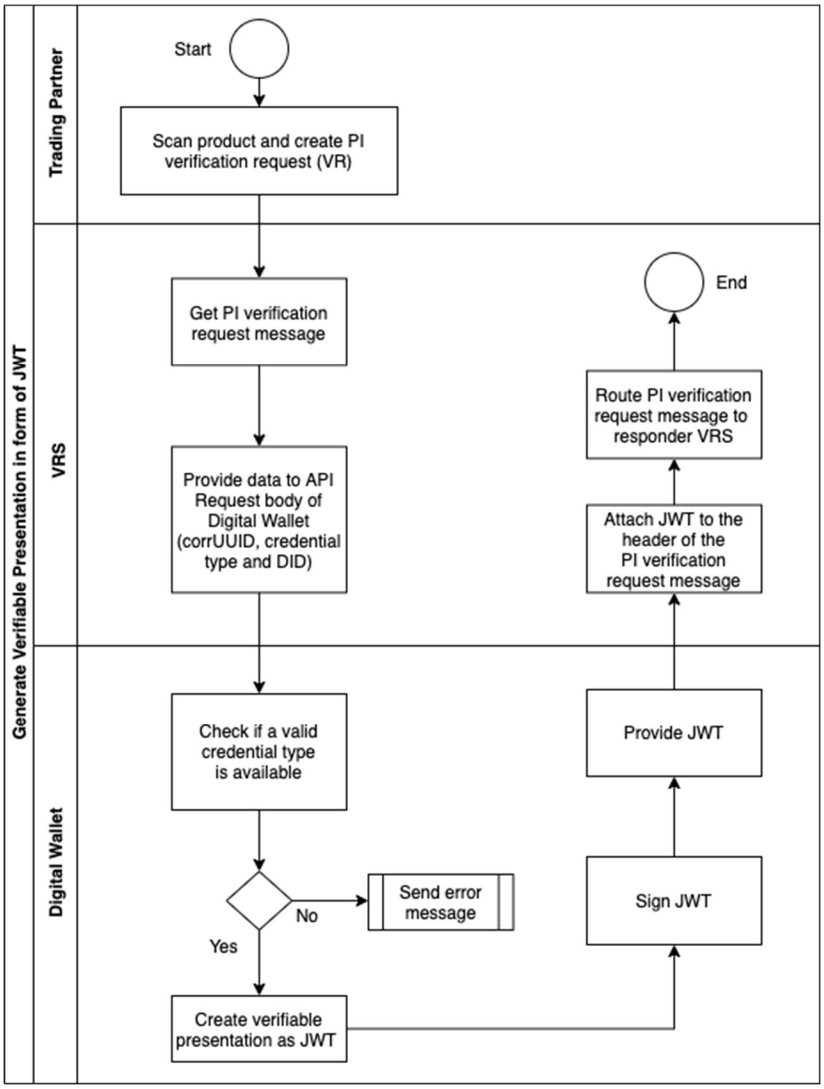

Figure 11a - Illustration of generating verifiable credential use in PI Verification interactions.[28]

Verify an OCI-Conformant ATP Credential Presentation

The verification flow starts with the VRS sending the JWT and the verifier DID to the Digital Wallet of the trading partner receiving either a PI request or response message:

[28] OCI contribution

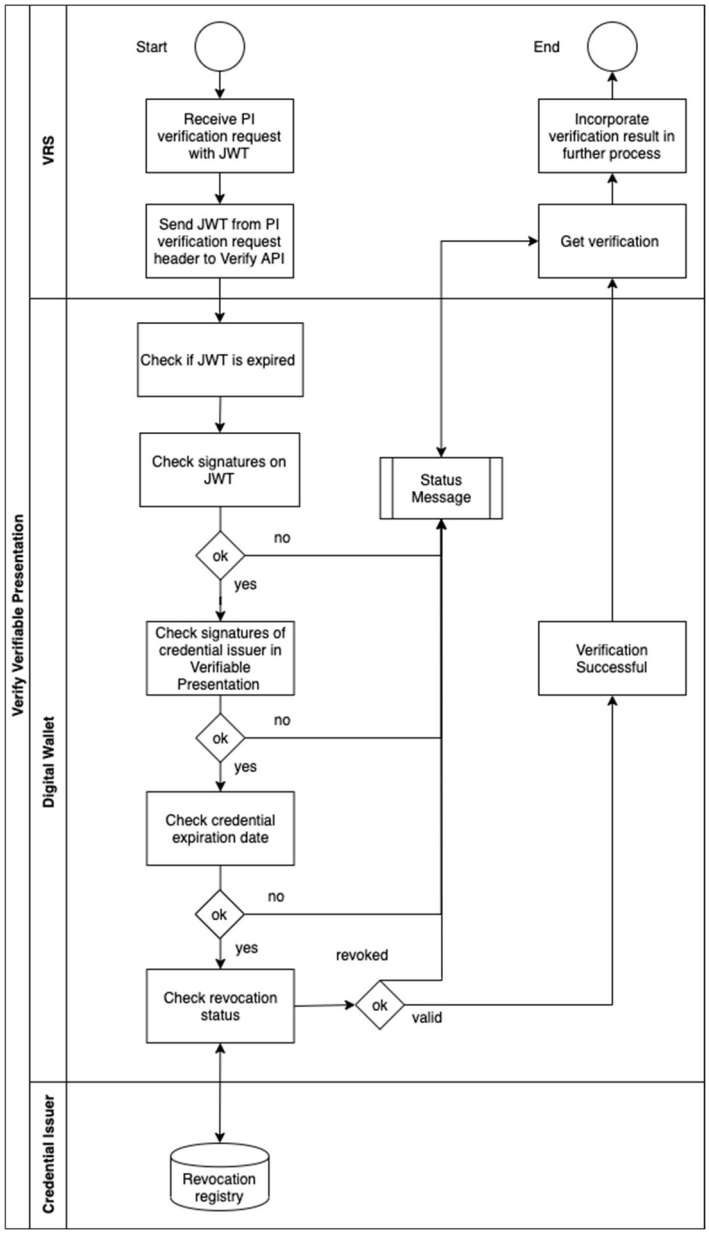

Figure 11b - Illustration of verifying a verifiable presentation use in PI Verification interactions.[29]

[29] OCI contribution.

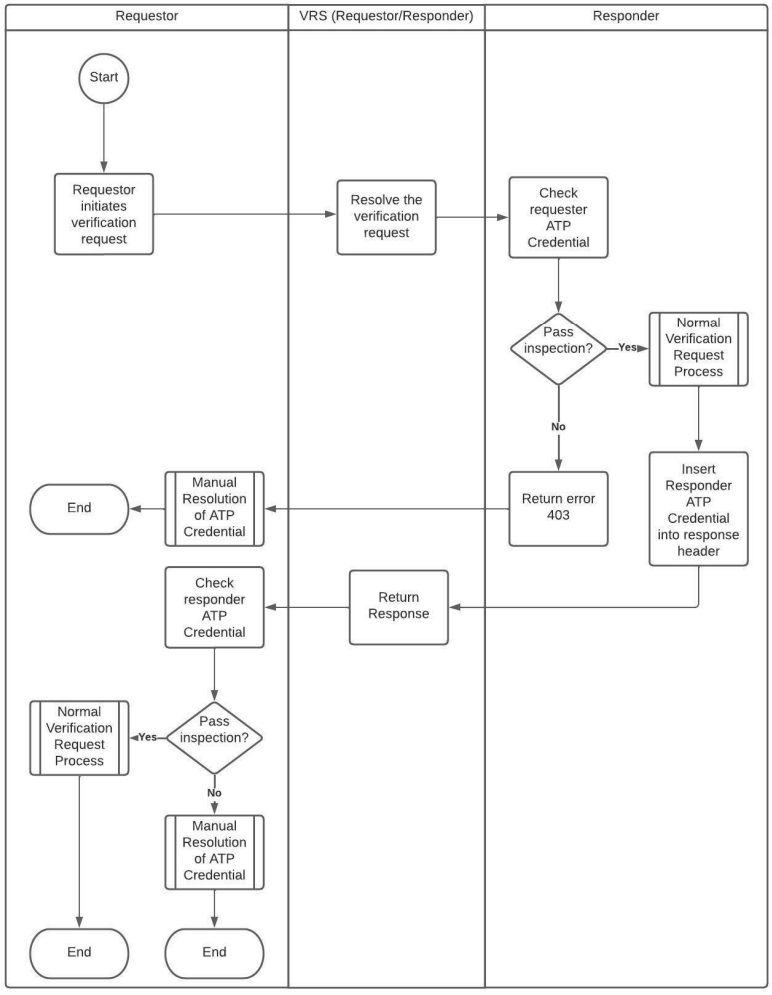

Figure 11c - Credential exception process illustration.

Digital Credentialing for Product Ownership Tracing

Interoperable TI Tracing will predominantly occur point-to-point using the message structure and choreography detailed in Chapter 5. TI requests and TI responses based on the PDG TI Request and TI Response messages for Interoperable TI Tracing are initiated with a trading partner and continued with other trading partners who have had ownership of the product. In this way, a participant in the PDG-defined EDDS network can request TI from adjacent and subsequent trading partners and gather documentation of the full path of ownership.

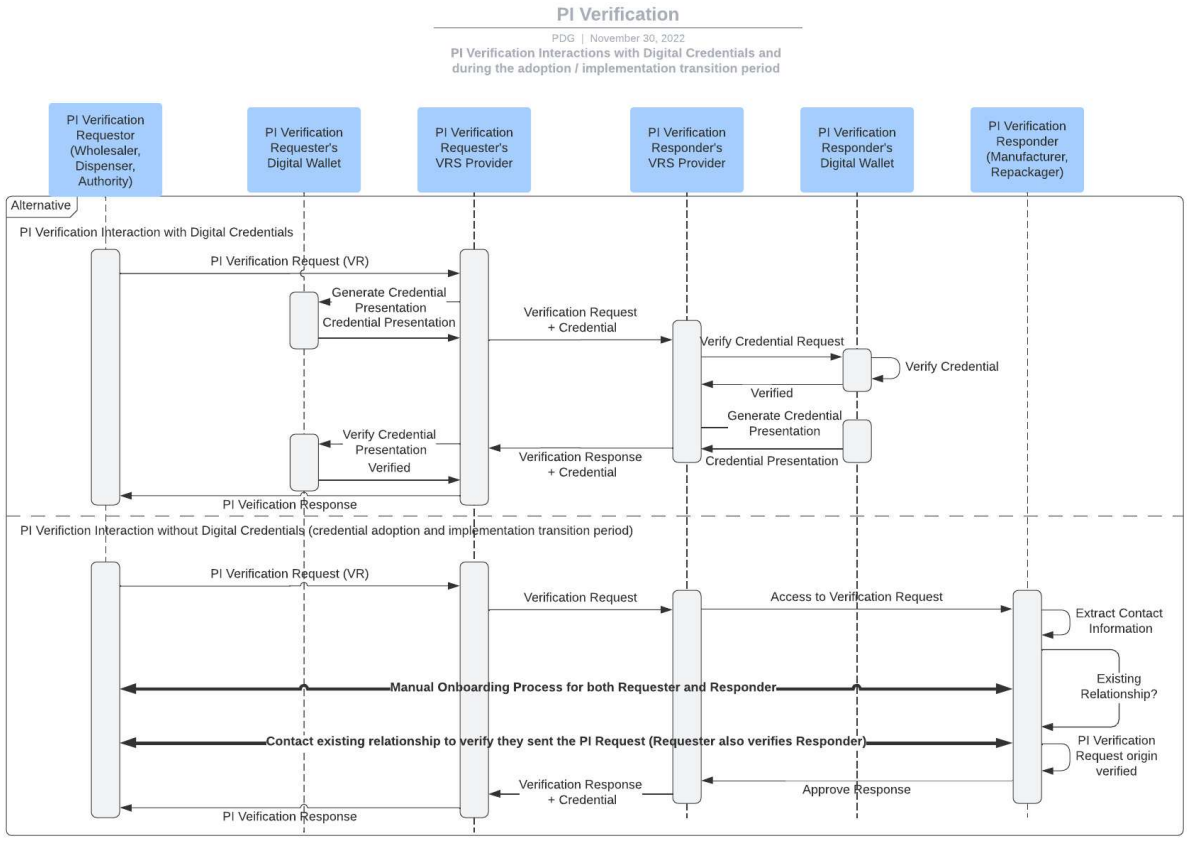

Figure 12 - Illustration - Authentication & Authorization for PI Verification Interactions

Functional Requirements

The PDG-defined EDDS network endorses and incorporates by reference the use of the W3C Verifiable Credential, Decentralized Identifier standards, and NIST identity proofing standard as implemented in compliance of the Open Credentialing Initiative (OCI) digital credential specifications for DSCSA PI-Verification and TI Tracing. Using these standards and specifications enables interoperability of authentication and authorization information between PI Verification and TI Tracing solutions within the PDG-defined EDDS network.

ID	Functional Requirement
Cred-FR-001	In the case where a valid State license is required to be considered an Authorized Trading Partner, ATP Credential Issuers SHALL issue ATP Credentials in accordance with Appendix 1 – State License Status.
Cred-FR-002	In the case where a valid State license is required as proof of an Authorized Trading Partner, ATP Credential Issuers SHALL revoke ATP Credentials in accordance with Appendix 1 – State License Status.
Cred-FR-003	No single vendor lock-in. Open specifications that allow for competition and vendor choice.
Cred-FR-004	Application of digital credentials to the PDG-Defined EDDS network SHALL be interoperable across the network.
Cred-FR-005	Credential Issuers SHALL be conformant with OCI conformance criteria[30]
Cred-FR-006	Digital Wallets Shall be conformant with the OCI conformance criteria[31]
Cred-FR-007	VRS Solutions Shall be conformant with the OCI conformance criteria[32]

Non-Functional Requirements

ID	Non-Functional Requirement
Cred-NFR-001	None

PDG-defined EDDS network, ATP-Equivalent and DSCSA Authority Parties

ATP-Equivalent Entities

The PDG membership recognizes that there are trading partners that are not required to register with the FDA or obtain a State license and as such will not be able to qualify for an ATP Credential. At the time of publication, PDG has requested that OCI create the specifications for an ATP-Equivalent digital credential

[30] https://www.oc-i.org/resources-portfolio/oci-interop-v2-0-0.
[31] https://www.oc-i.org/resources-portfolio/oci-interop-v2-0-0.
[32] https://www.oc-i.org/resources-portfolio/oci-interop-v2-0-0.

to support authentication and authorization during PI Verification and TI Trace electronic interactions. The following is an illustrative list of organizations anticipated:

- The Veterans Administration,
- The Department of Defense,
- Federal Prisons,
- The Bureau of Indian Affairs,
- Administration for Strategic Preparedness and Response (ASPR)/Strategic National Stockpile, and
- Tribal-operated dispensers.

The PDG membership is recommending that PDG maintain a list (in collaboration with industry and FDA) of recognized entities that qualify as an ATP-Equivalent. If at any point, the Secretary or Secretary's designee publishes a list of recognized ATP-Equivalents, PDG shall defer to that list.

The PDG-maintained list of ATP-Equivalents should be auditable, easily maintainable, and secure. Additionally, the removal or addition of ATP-Equivalent parties should not influence already issued and transacted credentials or their verifiability. Changes to the list must be trackable and auditable. Issuers of these credentials MUST monitor the list, review changes to the list, and revoke credentials of entities not on or represented by entities on the list.

DSCSA Authorities

The PDG membership recognizes that the Secretary and "other appropriate Federal or State officials" are empowered to perform PI Verifications and TI Traces. At time of publication, PDG has requested that OCI create the specifications for a DSCSA Authority digital credential to support authentication and authorization during PI Verification and TI Trace electronic interactions. The following is an illustrative list of organizations anticipated:

- FDA,
- State Licensing Authorities (ex: State Boards of Pharmacy), and
- DEA.

The DSCSA refers to authorities making information requests of trading partners as "the Secretary or other appropriate Federal or State official." The Credentialing WG is recommending that PDG maintain a list (in collaboration with industry and the FDA) of authorities that are recognized as meeting the DSCSA definition. If at any point the Secretary or Secretary's designee publishes a list of recognized DSCSA Authorities, that list will be the official, recognized list.

The PDG-maintained list of DSCSA Authorities should be auditable, easily maintainable, and secure. Additionally, the removal or addition of DSCSA Authorities should not influence already issued and transacted credentials or their verifiability. Changes to the list must be trackable and auditable. Issuers of these credentials MUST monitor the list, review changes to the list, and revoke credentials of entities not on or represented by entities on the list.

APPENDIX

Credentialing in TI/TS Exchange

TI/TS Exchange always occurs between Trading Partners that have already mutually determined each other's identity, ATP or ATP-Equivalent status, and their exchange of TI/TS is made using mutually agreed on exchange mechanisms. The result is that each party in a TI/TS exchange has confidence that the other party is who they claim they are (Authentication), have ATP or ATP-Equivalent status (Authorization), AND the information exchanged is transacted between these parties in the electronic exchange (trusted correlation and message integrity).

Extending the real-world Authentication and Authorization of a Trading Partner to the digital world of electronic interactions is accomplished for TI/TS exchange trading partners via their pre-exchange establishment of secure digital connections and trusted exchange systems and does not require the use of Digital Credentials.

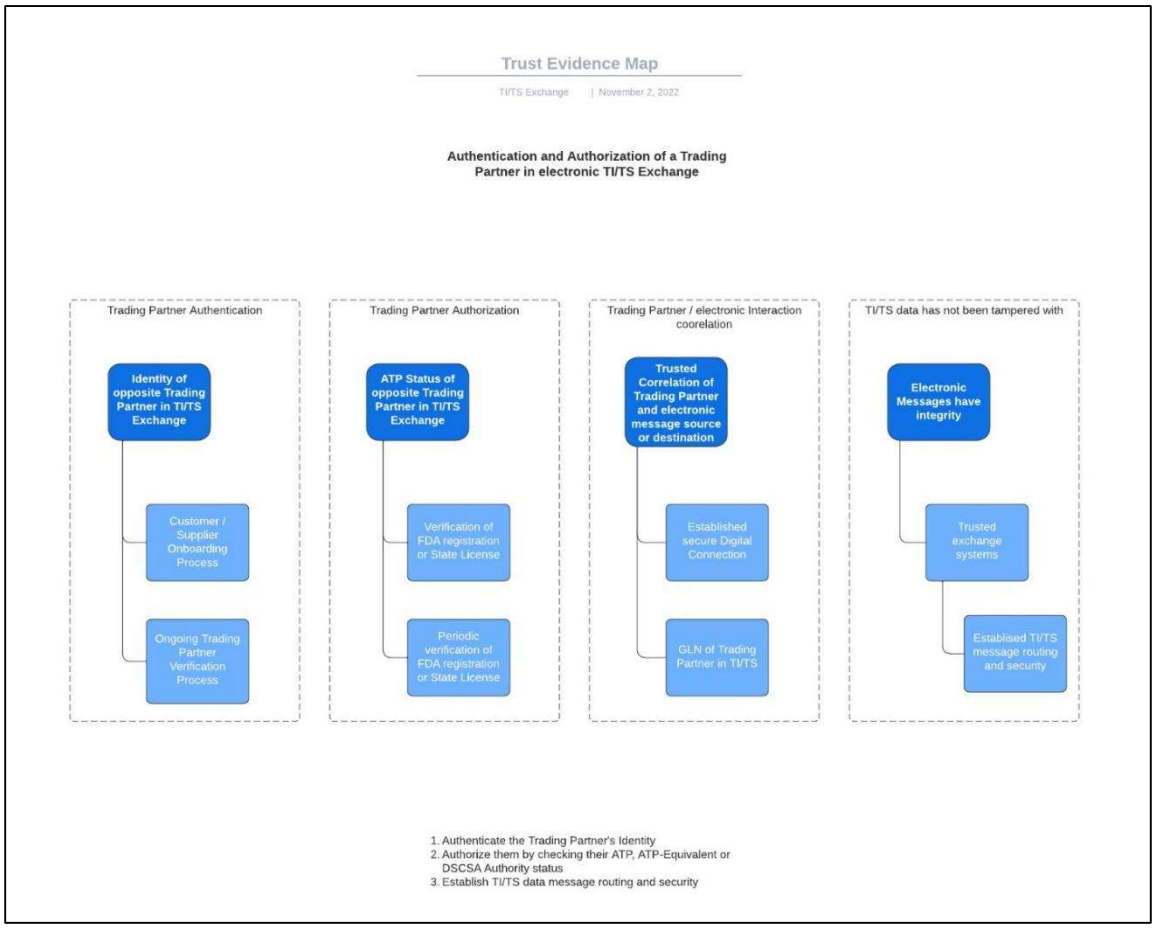

Figure 13 – Trust Evidence Map

Verifiable Credentials, Presentations, and Signatures

Each participating trading partner acquires and holds their Identity and ATP credential in their digital wallet (a software application/solution or internal solution). When a verifiable credential is used in a PI Verification or TI Tracing interaction, the verifiable credential is "wrapped" in a Verifiable Presentation (of that credential), which holds information about the usage as well as the trading partner's digital signature. It can be thought of as the Issuer's signature being used to verify and detect tampering with the credential and the trading partner's signature is used to verify the presentation of the credential and detect unwanted actions such as credential presentation replay (using a trading partner's credential outside of the trading partner's permission. The credential issuing process (within the Issuer's control) and the credential using process (within the digital wallet, PI Verification, and Trace solution control) are required to create and maintain audit records to be used by trading partners to assess the proper usage of their credentials.

Figure 14 illustrates the relationship between Verifiable Credentials, Verifiable Presentations, and the Issuer's and Trading Partner's digital signatures. This architecture provides resilience and mitigation features to compromises of Issuer and trading partner private keys.

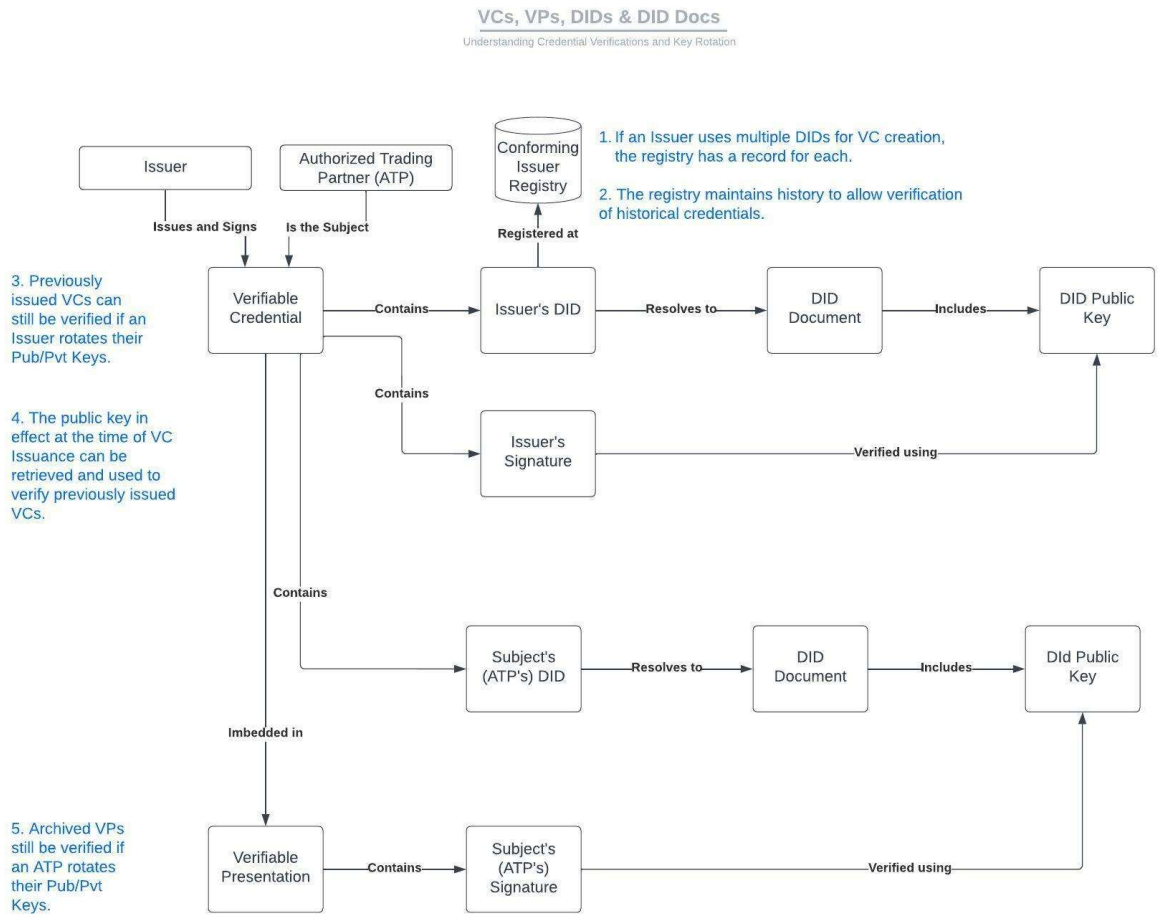

Figure 14 - Illustration of Verifiable Credentials, Verifiable Presentations and Signatures.

State Licensing Status and ATP Credential Issuance

The DSCSA requires that trading partners only transact with other trading partners that are "Authorized." In the case of Wholesalers and Dispensers, "Authorized" is defined as having a valid license under State law. There are several issues with licensing data across the various Boards of Pharmacy and other State regulatory agencies that will affect normalizing the issuance and maintenance rules for credentialing based on State license data.

Table 3 lists the current license statuses by State and the decision as to whether to issue an ATP credential based on that status. An interpreted Status of "Active" infers the trading partner is "Authorized." An Interpreted Status of "Non-Active" does not infer that the company is not an "Authorized" trading partner, rather, it depicts whether an ATP Credential Issuer would issue an ATP credential or revoke a current credential. An Issuer will issue an ATP credential if the Interpreted Status is "Active." An Issuer will revoke an ATP Credential when the Interpreted Status becomes "Non-Active."

Credentialing requirements documented in Chapter 1 require an ATP Credential Issuer to ensure certain trading partner types hold a valid State license. All ATP Credential Issuers SHALL only consider a trading partner an "ATP" if their State license status has a corresponding "Interpreted Status" of "Active" in *Table 3*.[33]

[33] This information has been approved by PDG membership and shared with FDA and State Boards of Pharmacy (through their association, NABP).

Change Control

Date of Change	Section	Description of Change	Approved By
Version 1.2			
		No changes from prior version	