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

Chapter 4: Product Identifier Verification Functional Design

Version 1.3
January 16, 2024

Table of Contents

Table of Figures

Chapter 4: PI Verification Functional Design

Product-Identifier[1] (PI) Verifications are executed to support saleable returns, suspect and illegitimate product investigations, recall processes, exception processing, or status checks. Within the PDG-defined Enhanced Drug Distribution Security System (EDDS) network, PI Verifications are executed as either a PI Verification Request and Response interaction between the Requester (Wholesaler, Dispenser, or authority) and the Responder (Manufacturer or Repackager) or by using TI and TS records received directly from the Manufacturer or Repackager (known as Direct-to-Replicate Verification) by Wholesalers. A PI Verification Requester may be a DSCSA-defined authorized trading partner (ATP), an industry-recognized trading partner (ATP equivalent), or an industry-recognized DSCSA Authority. There are many aspects to investigations driven by regulatory, legal, and business policy. A PI Verification Request results in information gathered to help in the investigation. For a suspect product or illegitimate product PI Verification Request, by its very nature, also provides the Responder with documented information that an investigation has been initiated.

Purpose of the document

This Product Identifier Verification Functional Design provides detailed information on *how* electronic PI Verification functional components of the PDG-defined DSCSA EDDS network operate. This document is created based on the high-level requirements for PI Verification (Chapter 1), the functional requirements, existing requirements, constraints, guidelines, and specifications of both the Healthcare Distribution Alliance (HDA) and GS1 US, recommendations of the PDG PI Verification Work Group, and agreed to by the PDG membership. Included in this section are detailed functional requirements including use cases, system inputs and outputs, process flows, diagrams, and sample PI Verification scenarios.

Terms/Acronyms and Definitions

Term/Acronym	Definition	Notes
Direct-to-Replicate Verification	A product identifier could be verified against a replicate of the commissioning-level data generated by and received from the Manufacturer or Repackager of the product.[2]	
Direct-to-Source	A product identifier could be verified against commissioning-level data generated and maintained by the Manufacturer or Repackager of the product.[3]	
LVMS	Lightweight Verification Messaging Standard published by GS1 US (see *Standards, Specifications, and Guidance*),	

[1] Product Information includes the NDC, Lot Number, Serial Number, and Expiration Date.
[2] PDG *Blueprint*, Chapter 1, Verification Methods.
[3] PDG *Blueprint*, Chapter 1, Verification Methods.

Partnership for DSCSA Governance

Standards, Specifications, and Guidelines

The following standards, specifications, and guidelines are pivotal to the proper implementation of product information verification, specifically, the GS1 US Implementation Guideline for Applying the GS1 Lightweight Messaging Standard for DSCSA Verification.

Reference Document	Version	Publisher	Notes
Implementation Guide: Applying the GS1 Lightweight Messaging Standard for DSCSA Verification of Product Identifiers	Release 1.3 October 5, 2022	GS1 US	Lightweight Messaging Standard for DSCSA Verification (LVMS)
Implementation Guideline: Applying GS1 Standards for DSCSA and Traceability	Release 1.2, 2016-11-07	GS1 US	
VRS Business Requirements Document	Version 3, 2019-04-12V3	HDA	
Verification Router Service (VRS) Solution Architecture Reference Document	Version 2, 2019-04-12	HDA	
VRS Technical Specifications for Responder CI Upload to Look Up Directory and LD Synchronization	Version 1.10, 2018-09-12	HDA	
Solution Architecture Reference Document	Version 2, 2019-04-12	HDA	
Current Security Approach		HDA	
Verifiable Credential Resources		W3C, OCI	See Chapter 6, Credentialing and User Authentication for a list of standards and open specifications this chapter relies on

PI Verification Functional Design Overview

As defined in Chapter 1 of the PDG *Blueprint*, the following methods of verifying a Product Information (PI) have been identified for use within the PDG-defined EDDS network. Chapter 1 also defines the business requirements for the use of these methods.

Direct-to-Replicate Verification

Chapter 3 of the PDG *Blueprint* defines the functional architecture for exchanging or making available DSCSA Transaction Information and Transaction Statements (TI and TS). *Figure 1* and *Figure 2* provide illustrative examples of a trading partner that has received TI and TS data directly from the Manufacturer or Repackager using those records to verify the product in their possession. This direct-to-replicate verification is an appropriate method of verification for saleable returns in the circumstances described in Chapter 1.[4] In this method, the trading partner verifies the Product Identifier (NDC/GTIN, Lot Number, Serial Number, and Expiration Date) directly against the TI and TS records they have received or have access to from the Manufacturer or Repackager.

Direct-to-Source Verification

The PDG-defined EDDS network endorses and incorporates by reference the use of the GS1 Lightweight messaging standard as implemented in compliance with the GS1 US Implementation Guideline – Applying the GS1 Lightweight Messaging Standard for DSCSA Verification of Product Identifiers.[5] Using this standard and guideline enables interoperability of PI Verification solutions within the PDG-defined EDDS network. HDA has developed extensive documentation to support the establishment of a Verification Router Service (VRS) and Look-up Directory (LD) synchronization to support a standard protocol for Manufacturer and Repackager verification endpoint (connectivity information) sharing by participants in the VRS ecosystem. The PDG-defined EDDS network endorses and incorporates by reference the HDA VRS requirements and design specifications.[6]

Figure 1 illustrates Direct-to-Source Verification utilizing message routing functionality. This functionality is defined in the HDA Verification Router Service Solution Architecture Reference Document and referenced in the GS1 US Implementation Guide (see *Standards, Specifications, and Guidelines*).

Figure 2 illustrates Direct-to-Source Verification utilizing message exchange directly between Verification services. This functionality is also defined in the HDA Verification Router Service Solution Architecture Reference Document and referenced in the GS1 US Implementation Guide (see *Standards, Specifications, and Guidelines*).

Establishing Connectivity Among PI Verification Solutions

Both methods of Direct-to-Source Verification require the verification requester to know the endpoint or connectivity information of the verification responding service for the GTIN of the product being verified. The HDA VRS Technical Specifications for Responder CI[7] Upload to Look-up Directory and LD Synchronization (see *Standards, Specifications, and Guidelines*) provides the messaging protocol and message structure for synchronizing verification responder (Manufacturer/Repackager solution) connectivity information across participating Look-up Directory solutions. The Look-up Directory defines the verification responder service connection endpoint by GTIN as maintained by the respective Manufacturer/Repackager.

---

[4] PDG *Blueprint*, Chapter 1, Requirement-Ver-001.
[5] This Implementation Guide is also applicable to Product Information Verification for the purposes of Saleable Returns, Suspect, Illegitimate and Recalled Product investigations.
[6] See *Standards, Specifications and Guidelines.*
[7] CI: Connectivity Information.

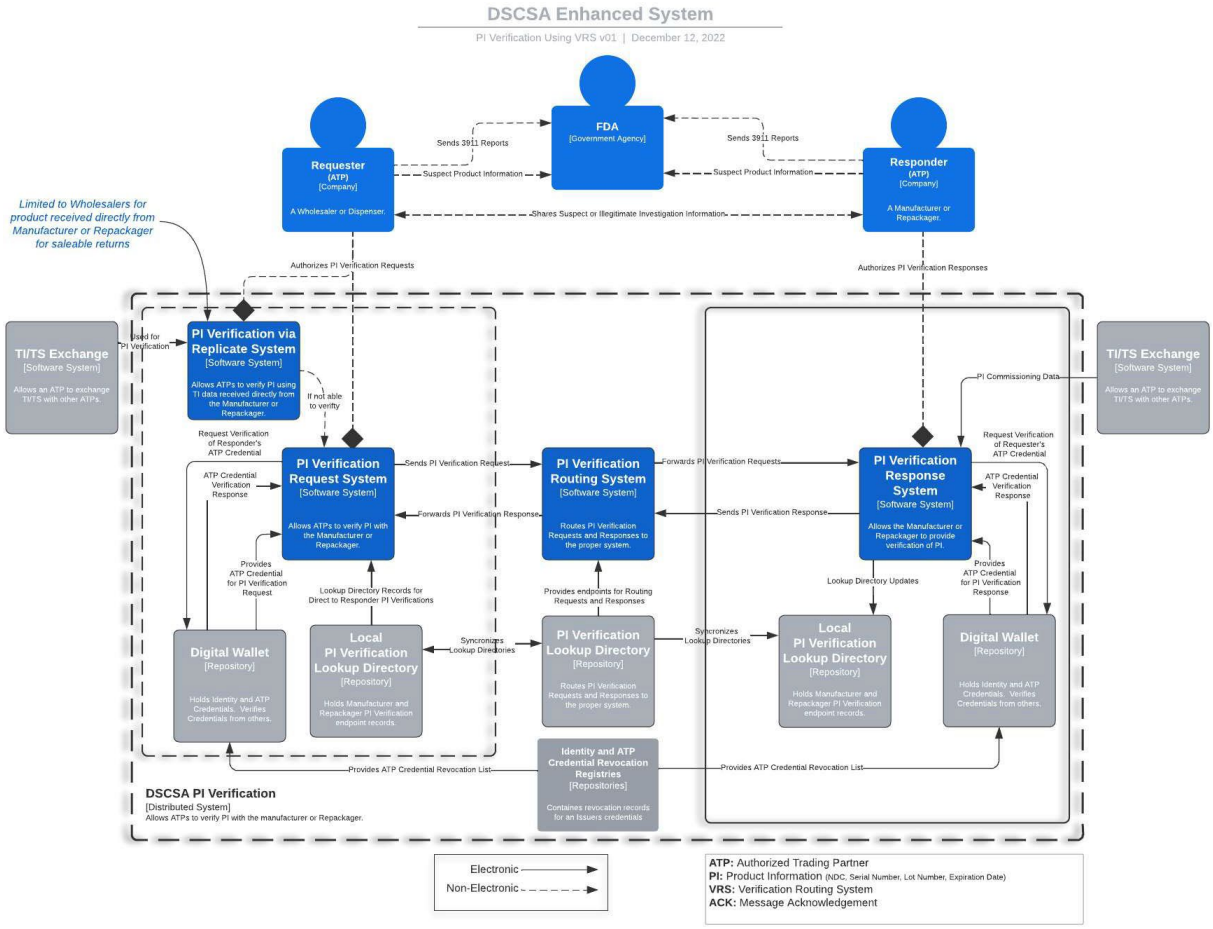

Figure 1 – PI Verification Request is routed to another VRS solution using the LD connectivity information.

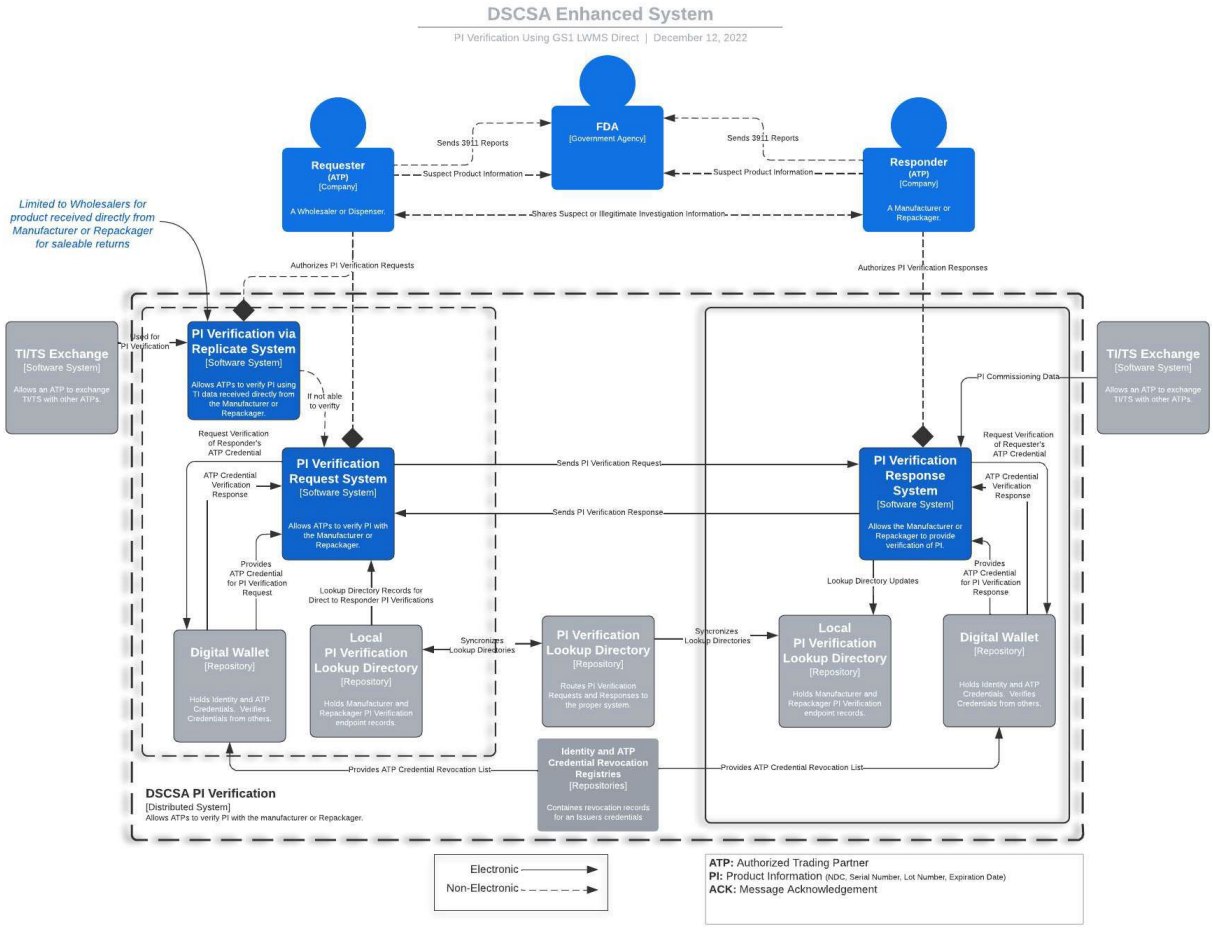

Figure 2 – PI Verification without the need to route the request to another VRS solution.

PI Verification and Interoperability

Figures 3a and 3b illustrate the interactions, standards, and methods that are needed to maintain interoperability within the PDG-defined EDDS network. For the purposes of PI Verification, we concentrate our attention on the PI Verification (blue) interactions augmented by the Credentialing (blue) interactions as the primary method for most network participants to perform direct-to-source verifications in an interoperable way. TI and TS exchange data sets (grey) can be used by trading partners that directly purchase products from Manufacturers or Repackagers in those instances where direct-to-replicate verification is appropriate.

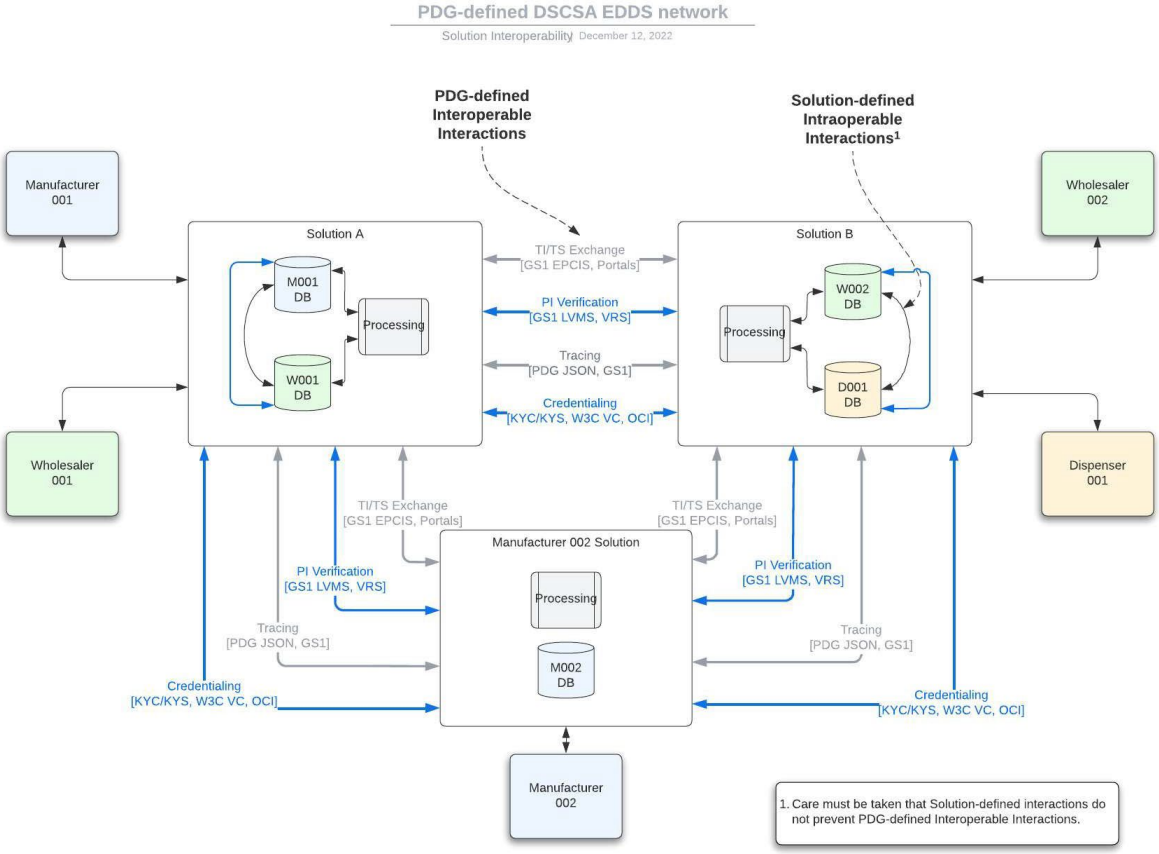

Figure 3a - PI Verification and Interoperability.

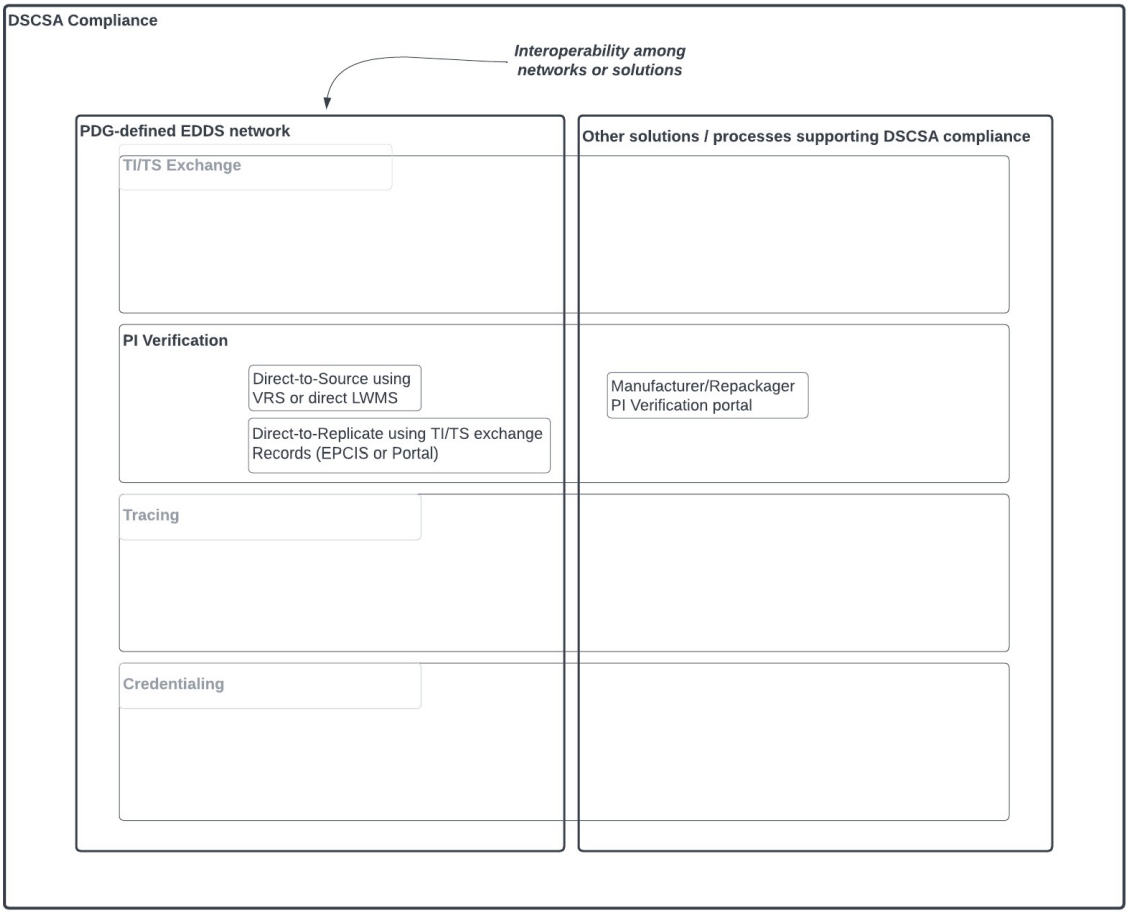

Figure 3b - Illustration of PDG-defined EDDS network design and other supporting solutions.

Illustrative PI Verification Choreographies

Direct-to-Replicate PI Verification. *Figure 4* depicts a Wholesaler that purchased product directly from the Manufacturer/Repackager using Manufacturer/Repackager supplied TI and TS Data to verify the Product Identifier of returned product. As noted above, this design is for illustrative purposes only, as a trading partner may structure its internal processes for direct-to-replicate verification to meet its business needs.[8]

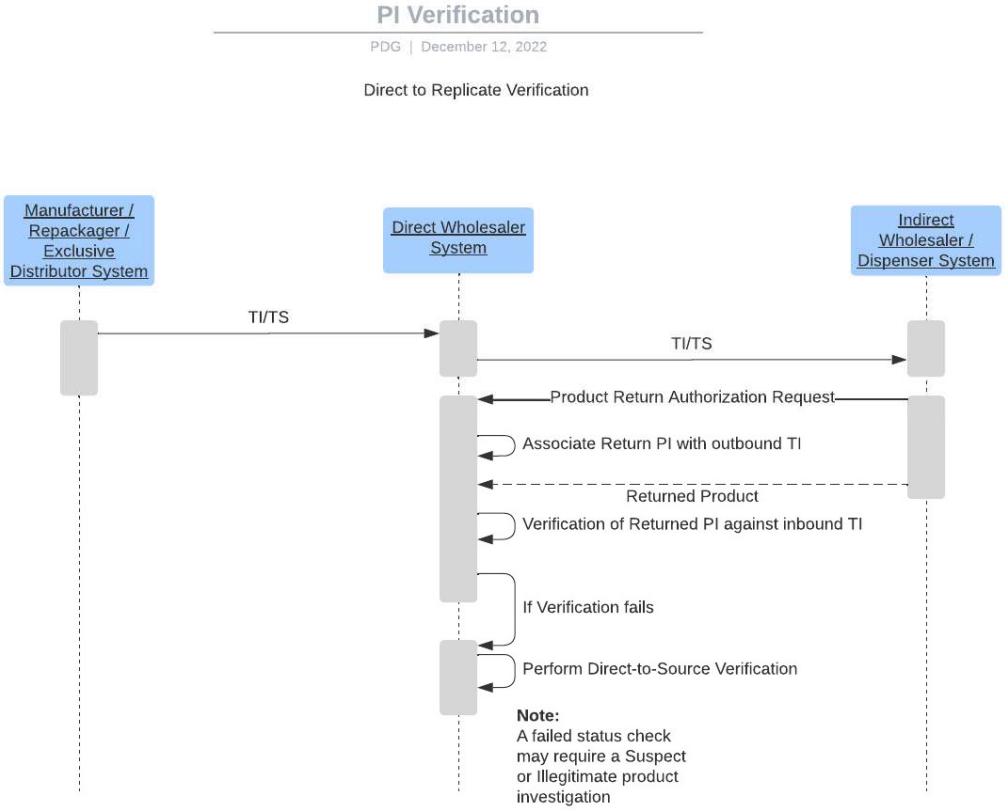

Figure 4 - Using Manufacturer / Repackager TI and TS data to verify direct-purchase products for Saleable Returns.

[8] See Chapter 1 for Direct-to-Replicate business requirements.

Direct-to-Source PI Verification. *Figure 5* Illustrates a PI Verification Request through PI Verification Response interaction between Requestors and Responders and their associated VRS or direct Lightweight Verification Messaging Standards (LVMS) solutions. A VRS[9] solution may route PI Verification Requests and Responses to members of their network (or the member's solutions); however, the PI Verification Request and Response messages remain intact throughout the routing process.

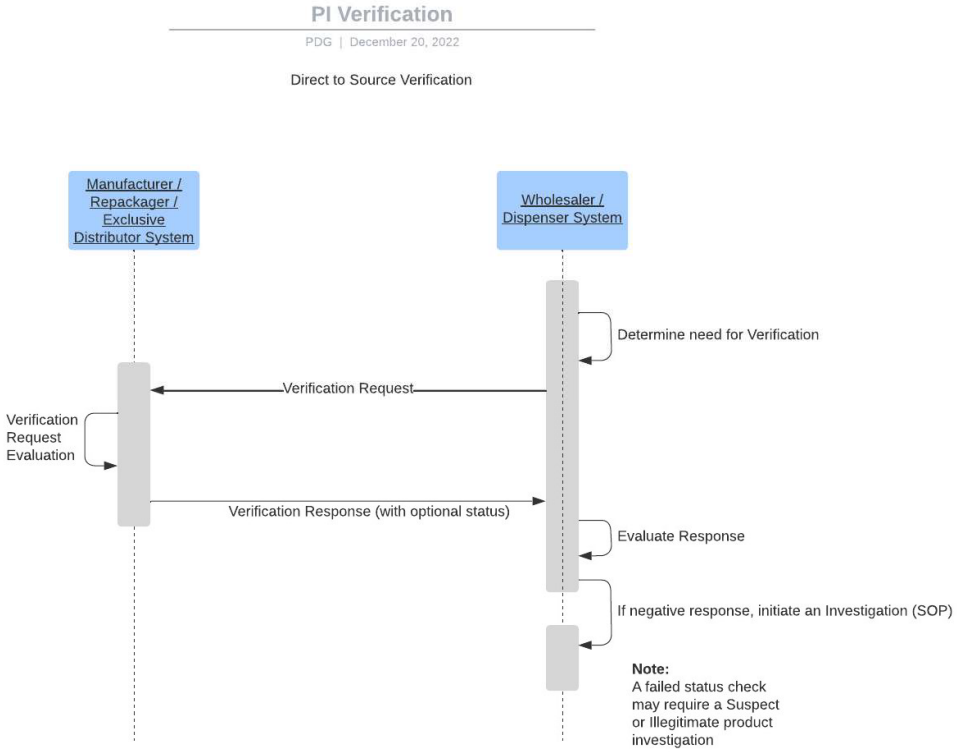

Figure 5 - Direct-to-Source: PI Verification (Illustration).

Using Verifiable Credentials for PI Verification Interactions

The DSCSA requires Manufacturers and Repackagers to interoperably respond to verification requests from trading partners that are "Authorized."[10] Also, interacting in a highly distributed network such as the PDG-defined EDDS network requires trading partners to ensure the identity of the other party in the interaction. The PDG-defined EDDS network endorses and incorporates by reference the use of W3C Verifiable Credentials as implemented by the OCI open specifications. Section 3.3 Security Considerations of The GS1 US Implementation Guide – Applying the GS1 Lightweight Messaging Standard for DSCSA Verification of Product Identifiers[11] provides for the use of digital credentials that are defined in Chapter 6 of this *Blueprint*. *Figure 6a* illustrates the use of credentials in the PI Verification process.

[9] VRS Providers provide PI Verification Request service, PI Verification Response service, and Lookup Directory service. Full stack VRS Providers provide all these services, but each VRS Provider can vary in the scope of services offered.
[10] See Chapter 1 Glossary for a definition of "Authorized."
[11] See *Standards, Specifications, and Guidelines*, this document also applies to PI Verifications for suspect, illegitimate, and recalled investigation purposes.

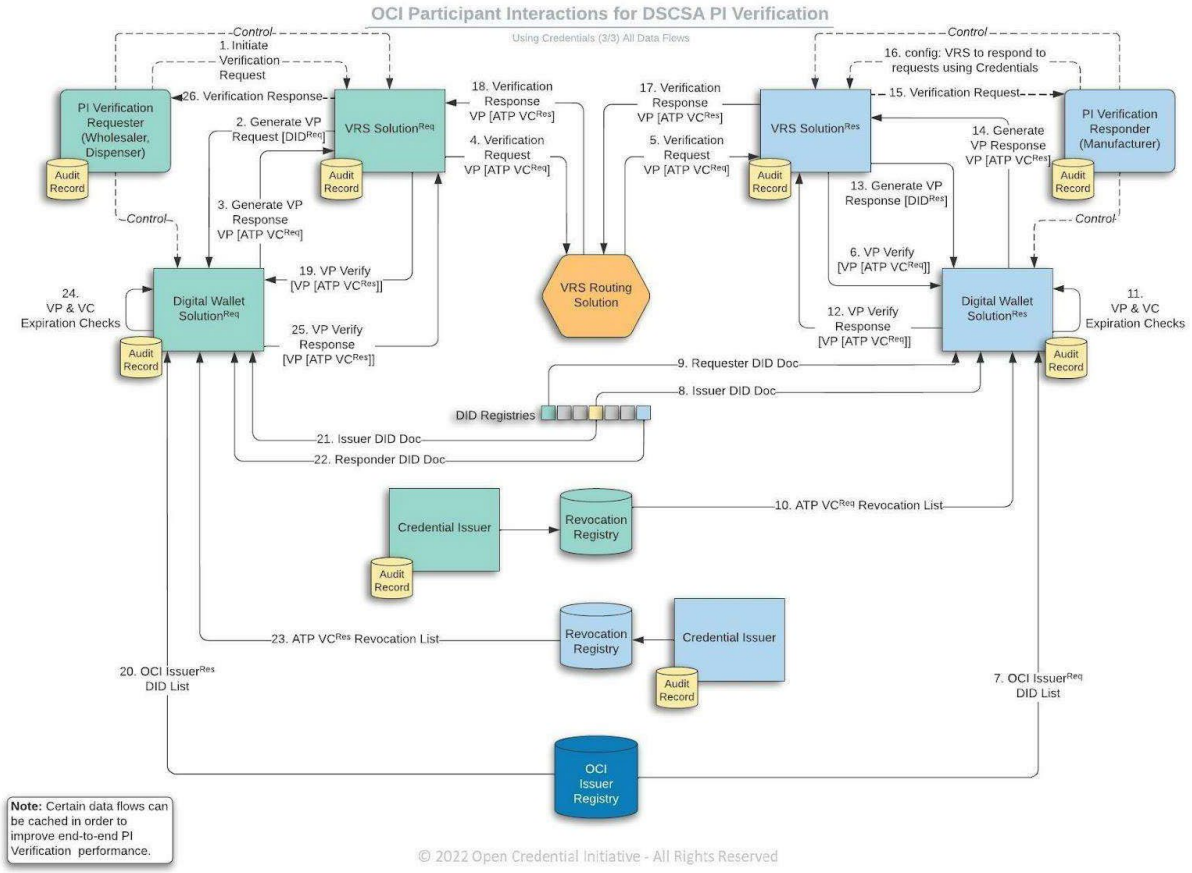

Figure 6a - Using W3C Standard Verifiable Credentials in PI Verification Requests and Responses and VRS.

PI Verification Interactions with Digital Credentials and Transition Period

Chapter 6 defines the digital credentials adopted for use in the PDG-defined EDDS network to digitally demonstrate authorized status according to the DSCSA and the PDG-defined credentialing process.[12] It is recognized that there will be a transition period within which participants in the PDG-defined EDDS network will implement verifiable credentials[13] for inclusion with PI Verification requests and responses. *Figures 8b* illustrates the process differences between PI Verification interactions where trading partner PI Verification systems use digital credentials[14] and when digital credentials are not used. The benefits of digital credential use over manual authentication and authorization processes (economic, interoperability, assurance, and security) are expected to drive increased adoption and implementation of digital credentials.

[12] Chapter 1: "Requirements and Recommendations to Support Credentialing and Trading Partner Authentication."
[13] Chapter 6: Credentialing and User Authentication.
[14] Chapter 6: Credentialing and User Authentication.

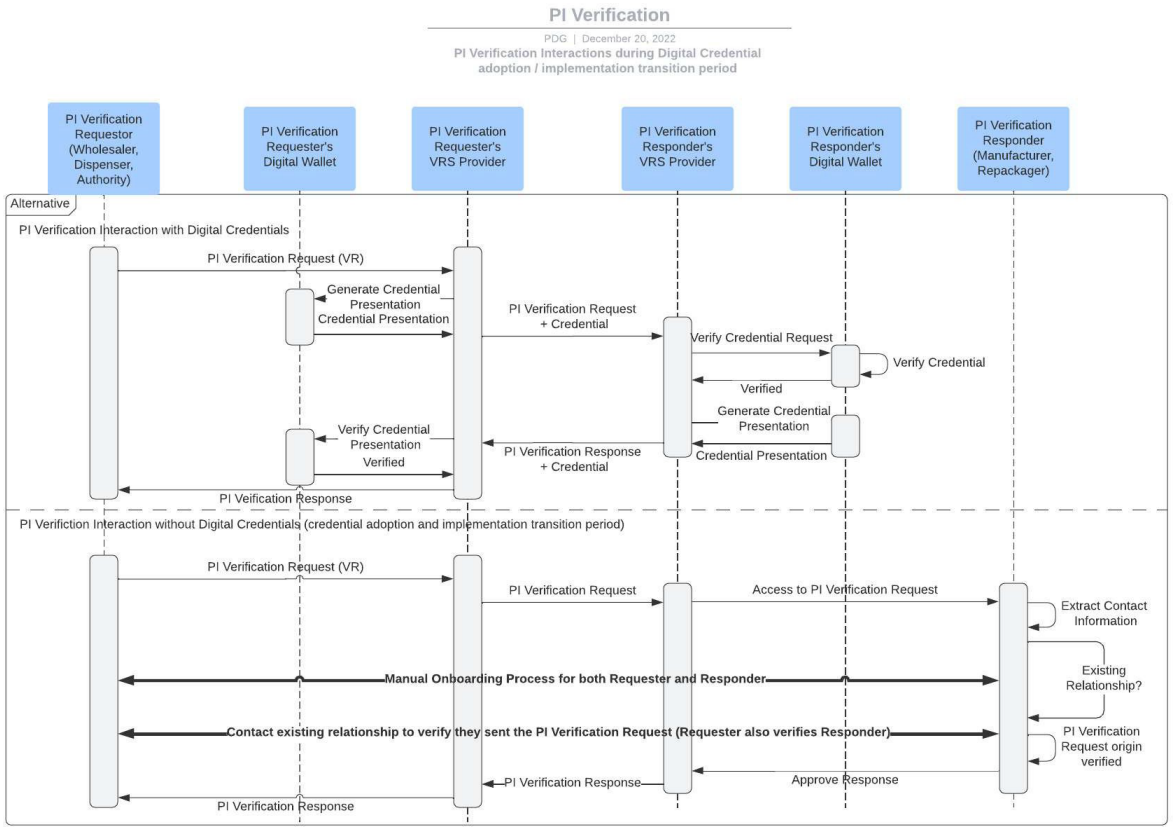

Figure 6b - PI Verification interactions with and without digital credentials.

Synchronizing Look-up Directories

PI Verification solutions in the distributed PDG-defined EDDS network must be able to determine the connectivity information of the solution that can receive and respond to PI Verification Requests. *Figure 7* illustrates[15] the interactions between Manufacturers/Repackagers, their VRS solutions, and other VRS solutions within the network. Synchronization of the GTIN connectivity information between Look-up Directories of VRS solutions in the network is done according to VRS Technical Specifications for Responder CI Upload to Look Up Directory and LD Synchronization.

[15] VRS Providers may provide PI Verification services, Lookup Directory services, or both.

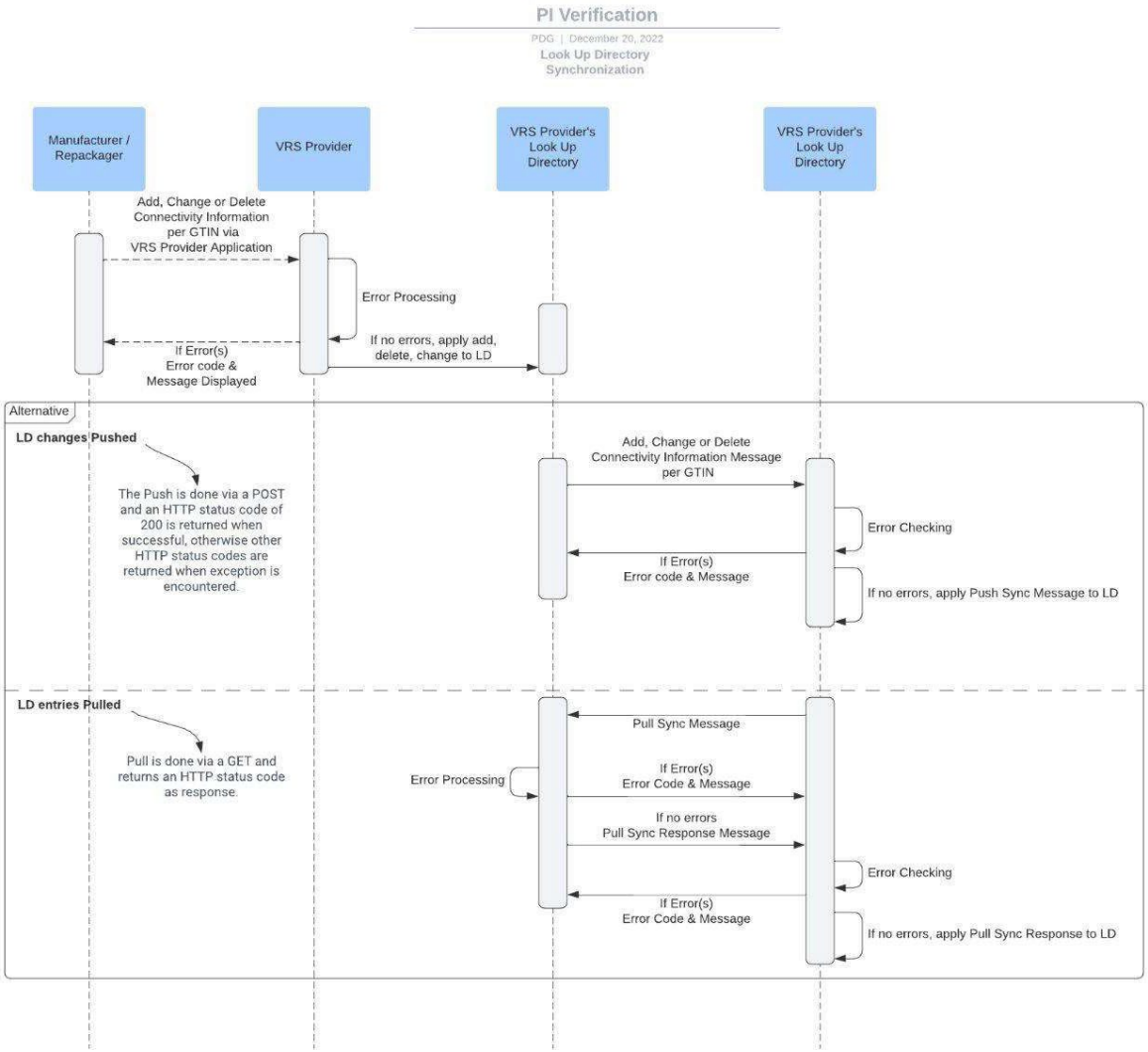

Figure 7 - Synchronizing Lookup Directory Connectivity Records.

Exception Processing

The GS1 US Implementation Guide for DSCSA Verification[16] and section 1.4.1 and 1.4.2 of the HDA LD Sync Specification[17] provides a list of HTTP status codes responses for exceptions when processing connectivity or verification requests as well as potential resolution paths to aid the Requester in correcting and resubmitting PI Verification requests. The Guide provides specific error codes and meanings. Additionally, the PI Verification Request and Response messages carry contact information for the Requester and Responder. This contact information can be used by the parties involved in a PI Verification interaction to resolve any issue that the GS1 US Guide exception process does not cover.

[16] See *Standards, Specifications, and Guidelines*.
[17] See *Standards, Specifications, and Guidelines*.

Functional Requirements

The documents listed in the *Standards, Specifications, and Guidelines* section contain functional requirements for PI Verification interactions and Look-up directory synchronization. Functional requirements listed below are added for PI Verification functionality within the PDG-defined EDDS network.

ID	Functional Requirement
Ver-FR-001	Look-up directories and resolvers MUST manage changes in Manufacturer or Repackager ownership of the product. In the case of a merger or acquisition, they MUST retain PI Verification Responder endpoint data for the past product (6 years) as well as provide access to the current PI Verification Responder endpoint.
Ver-FR-002	Look-up Directory solutions Shall provide the functionality to add new GTIN records per Verification Router Service (VRS) Solution Architecture Reference Document.
Ver-FR-003	Look-up Directory solutions Shall provide the functionality to maintain GTIN records per Verification Router Service (VRS) Solution Architecture Reference Document.
Ver-FR-004	Look-up Directory solutions Shall provide the functionality to exchange GTIN records with other Look-up Directory solutions per Verification Router Service (VRS) Solution Architecture Reference Document.
Ver-FR-005	For Direct-to-Source verification, solutions SHALL use either VRS or direct interaction using the LVMS (as specified in the GS1 US LVMS Implementation guideline)[18].

Non-Functional Requirements

The documents listed in the *Standards, Specifications, and Guidelines* section contain functional requirements for PI Verification interactions and Look-up directory synchronization. Non-functional requirements listed below are added for PI Verification functionality within the PDG-defined EDDS network.

ID	Non-Functional Requirement
Ver-NFR-001	None

[18] Manufacturers and Repackagers may also provide portals for PI Verification purposes outside of the PDG-defined EDDS network.

Change Control

Date of Change	Section	Description of Change	Approved By
Version 1.2			
2/21/2023	Ch. 4	Removed “Returned,” consistent with R1.3	PDG General Membership
2/21/2023	Ch. 4 Introduction	Added reference to exception processing and status check	PDG General Membership
Version 1.3			
8/28/2023	Ch. 4	Replaced “TI/TS” with “TI and TS”	PDG Board of Directors