

Verification Router Service (VRS)

Solution Architecture Reference Document

Version: 2

Date: 12-APR-2019

Table of Contents

| | | |
|----------|---|----|
| 1.0 | Introduction..... | 3 |
| 1.1 | Background..... | 3 |
| 1.2 | Purpose..... | 4 |
| 1.3 | Glossary..... | 5 |
| 2.0 | Solution overview | 7 |
| 2.1 | Business Processes..... | 7 |
| 2.2 | Functional Overview | 7 |
| 3.0 | Solution Architecture | 10 |
| 3.1 | Solution Architecture Components | 10 |
| 3.2 | Solution Architecture Interactions | 11 |
| 3.3 | Solution Architecture Illustrations | 12 |
| 3.4 | Communications Protocol & Data Elements for Interactions..... | 15 |
| 3.4.1 | Interaction 1:..... | 15 |
| 3.4.3 | Interaction 4:..... | 15 |
| 3.4.4 | Interaction 5:..... | 15 |
| 3.4.5 | Interaction 6:..... | 15 |
| 3.4.6 | Interaction 7:..... | 16 |
| 3.4.7 | Interaction 8:..... | 16 |
| 3.4.8 | Interaction 9:..... | 16 |
| Appendix | | 17 |
| 4.0 | Assumptions | 17 |

1.0 Introduction

1.1 Background

The Drug Supply Chain Security Act (DSCSA), enacted on November 27, 2013 in Title II of the Drug Quality and Security Act (DQSA), amends the federal Food, Drug and Cosmetic Act (FDC Act)¹ and establishes the requirement for implementation of an interoperable electronic system between trading partners which identifies the individual units of prescription drugs involved in a transaction where a change in ownership occurred. This legislation, which preempts state and local laws, mandates that all trading partners in the supply chain be authorized and hold appropriate licenses or registrations, details requirements for verification procedures and defines the information necessary to identify the distribution of prescription products down to the smallest unit intended for sale. This interoperable electronic system is to be implemented in stages over the next six years across the entire pharmaceutical supply chain. By November 27, 2023, each package of applicable prescription drug product must bear a product identifier², which includes a unique serial number³ that will link each saleable product unit to the selling and purchasing sources of the product in a secure, interoperable, electronic system [See § 582(g)(1)].

One important milestone in the progress towards the 2023 deadline and full product traceability begins on November 27, 2019.

Beginning on November 27, 2019, before it may resell a returned product, “the wholesale distributor shall verify the product identifier, including the [SNI] ... for each sealed homogeneous case or on each package” [§ 582(c)(4)(D)].

“Verification” or “verify” means “determining whether the product identifier affixed to, or imprinted upon on a package or homogeneous case corresponds to the [SNI] ... assigned to the product by the manufacturer or the repackager...”⁴ [§ 581(28)]. A manufacturer who receives a verification request from a repackager, wholesale distributor, or dispenser must respond to that request within 24 hours (or such other time the Food and Drug Administration (FDA) establishes) [§ 582(b)(4)(C)]. A repackager also has 24 hours to respond [§ 582(e)(4)(C)].

¹ Citations that follow to sections 581 and 582 refer to sections of the FDC Act as amended by the DSCSA and are codified at 21 U.S.C. § 360eee and §360eee-1, respectively.

² The product identifier requirement begins November 27, 2017, by which time manufacturers must affix or imprint a product identifier to each package and homogenous case intended to be introduced in a transaction into commerce [§ 582(b)(2)(A)]. However, the Food and Drug Administration has granted enforcement discretion and extended the date to November 27, 2018 for manufacturers. Repackagers must affix product identifiers a year later, by November 27, 2018. [§ 582(e)(2)(A)].

³ The product identifier is a standardized graphic in human-readable form and on a machine-readable carrier that conforms to international standards and includes the product’s unique standardized numerical identifier (SNI), lot number and expiration date [§ 581(14) (definition of product identifier); § 581(20) (definition of SNI)].

⁴ Section 581(28) also permits verification of a product identifier by “lot number and expiration date.” However, once all product is serialized, there would be no reason for trading partners to verify product by lot number and expiration date when the product identifier (which includes the SNI, lot number, and expiration date (§ 581(14)) would be more accurate and efficient.

1.2 Purpose

Healthcare Distribution Alliance (HDA) formed the Traceability Pilots Work Group to focus on a pilot study of nine (9) potential methods or solutions to meet the 2019 Saleable Returns DSCSA Requirements. Through the process of evaluating nine scenarios, the Work Group acknowledged no single solution for the supply chain existed, and put forward two preferred options, keeping in mind solution cost, implementation effort, process execution, exception handling, and other advantages and disadvantages. One of the options studied in the pilot was a Verification Router Service (VRS). A proof of concept was successfully built and utilized during a live pilot, but it was only a temporary system for the purpose of the pilot. (For the full pilots report, see <https://healthcaredistribution.org/resources/hda-saleable-returns-pilots-report>.) At the conclusion of the pilot study, the Work Group concluded that the Verification Router Service was a verification method worth pursuing.

HDA subsequently formed a task force consisting of industry members and later expanded to include solution providers. The task force developed business requirements for the Verification Router Service which were approved by HDA and published July 2017. HDA, working with KPMG LLP and the task force members, subsequently conducted several virtual meetings in September 2017 and an in-person workshop October 3, 2017 in order to document the solution architecture components, their interactions, and various design and operational considerations. The resulting output served as the basis of this Solution Architecture Reference Document, which the task force defined with the underlying assumption that the operating environment would consist of multiple VRS providers operating in a distributed environment.

The purpose of this document is to present the Solution Architecture Reference Document developed by the task force. The intent of the Solution Architecture Reference Document is to provide a framework for defining the recommended VRS components and the interactions necessary to support compliance with the 2019 Saleable Returns DSCSA Requirements. Additionally, the architectural approach aims to be scalable to meet the business needs for a diverse network of manufacturers and wholesale distributors. While the driver behind development of the Verification Router Service is to support 2019 Saleable Returns Requirements, there is the potential for manufacturers to use such a solution to meet November 27, 2017 DSCSA requirement to verify whether the product identifier, including the SNI, corresponds to the product identifier the manufacturer affixed or imprinted to the product. [§ 582(b)(4)(C)].

This document has been updated as the result of technical specifications being defined which provide the field-level data in scope for each interaction.

1.3 Glossary

| Term / Acronym | Definition |
|-------------------------------|---|
| Connectivity Information (CI) | A general term used in this document to refer to the technical information (e.g. end-point URL, security certificates, authentication parameters) needed to establish connection with the responder's repository. The details of what this connectivity information entails will be further defined in the design phase. |
| DQSA | Drug Quality and Security Act |
| DSCSA | Drug Supply Chain Security Act, Title II of the DQSA. See full law here or information from the Food and Drug Administration (FDA) here . |
| FDC Act | Food, Drug and Cosmetic Act. See full law https://www.gpo.gov/fdsys/pkg/USCODE-2015-title21/pdf/USCODE-2015-title21-chap9.pdf here. |
| GCP | Global Company Prefix, a unique GS1 identification code for your company obtained through GS1. For additional information see here . |
| GLN | Global Location Number, a unique GS1 identifier for a company (location). |
| GS1 | GS1 is an international organization that develops and maintains standards for supply and demand chains across multiple sectors. For additional information see here . |
| GTIN | Global Trade Item Number, used to uniquely identify trade items that are priced, ordered, or invoiced at any point in the supply chain. For additional information see here . For U.S. Rx product, the National Drug Code or NDC number is embedded in the GTIN. For additional information on the NDC see here . |
| UUID (Transaction ID) | Globally unique identifier (guid) assigned to system transactions for logging, tracking, and reporting purposes. |
| LD | Look-up Directory which contains the Connectivity Information of the Responders' Repositories. It is expected that the LD will be an integrated component of each VRS. |
| PI | Product Identifier, defined by DSCSA as a standardized graphic that includes, in both human-readable form and on a machine-readable data carrier that conforms to the standards developed by a widely recognized international standards development organization, the standardized numerical identifier, lot number, and expiration date of the product. In this context it is used to reference its component data elements: 1) GTIN, 2) Serial Number, 3) Lot Number, and 4) Expiration Date |
| Repository | Repository refers to the Responder's system that stores PI data and relevant data in order to provide responses to verification requests. |
| Requestor | Entity that initiates the verification requests (e.g. distributor) |
| requestorGLN (Requestor ID) | The GS1 Global Location Number (GLN) a Requestor uses to identify themselves. |
| Responder | Entity responsible for providing response to verification requests (e.g. manufacturers, re-packagers) for specified GTIN(s) |
| responderGLN | The GS1 Global Location Number a Responder uses to identify themselves. |

| Term / Acronym | Definition |
|--------------------------------|---|
| (Responder ID) | |
| Response | The message/file returned from the Responder to indicate validity of PI |
| SNI | Standardized Numerical Identifier, defined by DSCSA as “a set of numbers or characters used to uniquely identify each package or homogenous case that is composed of the National Drug Code that corresponds to the specific product (including the particular package configuration) combined with a unique alphanumeric serial number of up to 20 characters.” § 581(20). For additional guidance, though it predates the DSCSA, see here . |
| Transaction ID | A unique value assigned to requests that are initiated within the VRS. This should be unique across all VRS and further defined during the detailed design phase. |
| VR | Verification Request |
| VRS | Verification Router Service |
| VRS Provider / VRS Provider ID | Entity offering a Verification Router Service solution (which is expected to include a LD as an integrated component). |

2.0 Solution overview

2.1 Business Processes

The business processes identified as part of the initial requirements document have been assigned to one of the following three categories: (1) Enabling/Other Processes; (2) Requesting Processes; and (3) Responding Processes.

2.2 Functional Overview

The Verification Router Service community is comprised of Requestors, Responders, VRS Providers, and a Governance Body (TBD). The solution as a whole is envisioned to function in the following manner:

| Actor – Step | Functional Responsibility |
|--|--|
| Responder – Set-up | Determine if your organization will be using a VRS solution provider to generate and deliver responses to verification requests. |
| | Define your system architecture, including integration with a VRS solution provider if your organization will be using one. |
| | Select a VRS Provider if your organization will be using one. |
| | Determine value for GLN and provide to your selected VRS Provider. |
| | Provide Connectivity Information (CI) for each GTIN in scope to your selected VRS Provider or a VRS Provider operating a Look-Up Directory (LD). |
| | Conduct connectivity / set-up testing and other testing as defined by your organization. |
| Requestor – Set-up | Determine if your organization will integrate an internal application with a VRS provider; use a VRS provider's web portal; or both. |
| | Select VRS Provider. |
| | Determine value for GLN and provide to your selected VRS Provider. |
| | Conduct connectivity / set-up testing and other testing as defined by your organization. |
| VRS Provider – Registration and Set-up | Provide single point of contact name, phone, and e-mail for inclusion in the listing of VRS Providers and establishing value for VRS ID. |
| | Obtain Connectivity Information for other VRS Providers with whom you will be exchanging data via Peer-to-Peer. |
| | Perform connection setup and testing with other VRS Providers as applicable based on your system topography (e.g. blockchain, peer-to-peer, both). |
| | Obtain Responder Connectivity Information (CI) directly from Responder and maintain in a Look-up Directory (LD) at Global Trade Item (GTIN) level. |



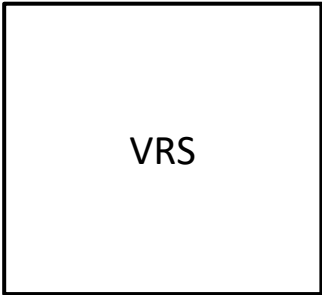

| Actor – Step | Functional Responsibility |
|--|--|
| | Synchronize Lookup Directory data with other VRS Providers using blockchain, peer-to-peer, or both as applicable. |
| Requestor - Initiate VR via interface to VRS Provider | Scan / Obtain the 4 data elements of the Product Identifier (PI) |
| | Create and format the Verification Request (VR) message / file, including generating a globally unique transaction ID (UUID), according to the GS1 Request and Response Messaging Standard |
| | Send the Verification Request (VR) to VRS Provider |
| | Record / Log the transmittal of the Verification Request (VR) |
| Requestor - Initiate VR using VRS Provider's Portal | Access the VRS Provider's portal via secure login |
| | Scan / Enter the 4 data elements of the Product Identifier (PI) |
| | VRS portal systematically generates a globally unique transaction ID (UUID) |
| | Initiate VR with assignment of globally unique transaction ID (UUID) previously generated |
| VRS Provider – Process VR | Receive VR from the Requestor |
| | Record / Log receipt of the VR from the Requestor upon successful security validation |
| | Determine Responder Connectivity Information (CI) or Responder's VRS Provider CI from the Look-up Directory (LD) based on the Global Trade Item Number (GTIN) from the PI provided by the Requestor. |
| | Update and format VR per GS1 Request and Response Messaging Standard. Route VR to Responder's Repository directly or to another VRS Provider as applicable. |
| | Record/Log the transmittal of the Verification Request to Responder or to another VRS as applicable |
| | Obtain Response to VR either directly from Responder or Responder's VRS Provider as applicable |
| | Record / Log Response from the Responder or Responder's VRS Provider as applicable |
| | Provide Response to Requestor via file/message (for scenario where Requestor uses internal system to initiate VR) or VRS display/message/report (for scenario where Requestor uses provider-portal to initiate VR) |
| | Record / Log delivery of Response to Requestor |
| Responder – Process VR | Receive VR from VRS Provider |
| | Record / Log receipt of VR upon successful security validation |

| Actor – Step | Functional Responsibility |
|---------------------------|---|
| | Determine Yes / No Response and if Optional information is to be provided Provide Response using GS1 Request and Response Messaging Standard format. Record / Log the event. |
| | |
| Requestor – Process VR | Receive Response to VR from VRS Provider Record / Log Response received from the VRS Provider |

3.0 Solution Architecture

3.1 Solution Architecture Components

The following table lists the main components of the VRS Solution Architecture:

| | |
|--|--|
|  <p style="text-align: center; color: blue; font-weight: bold;">REQUESTOR</p> | <p>The Requestor's System is used for the following processes*:</p> <ol style="list-style-type: none"> 1) Create verification request; 2) Submit verification request; and 3) Receive verification response |
|  <p style="text-align: center; color: orange; font-weight: bold;">RESPONDER</p> | <p>The Responder's System is used for the following processes*:</p> <ol style="list-style-type: none"> 1) Provide Connectivity Information (CI) to VRS Provider(s). 2) Receive verification request; 3) Formulate response; and 4) Provide verification response to requesting system |
|  <p style="text-align: center; font-weight: bold;">VRS</p> | <p>The Verification Router Service solution to be provided by multiple vendors, represented as P1, 2, ... n. The VRS is used for the following processes*:</p> <ol style="list-style-type: none"> 1) Receive request; 2) Route request to responder or responder's VRS; 3) Obtain response from responder or responder's VRS; and 4) Provide response to requestor |
|  <p style="text-align: center; color: purple; font-weight: bold;">LD</p> | <p>The Look-Up Directory which is envisioned to be an integrated component of the VRS. The LD is used for the following processes:</p> <ol style="list-style-type: none"> 1) Add new GTIN records; 2) Maintain GTIN records; 3) Exchange GTIN records with other VRS Providers. |

* Assumes security/authorization, transactional logging, and reporting functions are included as necessary and appropriate; scope of responder system processes will depend on whether responder uses a VRS

3.2 Solution Architecture Interactions

The following table lists the main interactions between the components of the VRS Solution Architecture:

| Interaction # | Process Category | Interaction Description |
|---------------|------------------|--|
| 1 | Enabling / Other | Connectivity Information (CI) provided by the Responder to multiple VRS Providers or one VRS Provider. |
| 2 | Enabling / Other | Exchange of VRS Provider ID used by Responder at GTIN level amongst VRS Providers for routing of VRs. |
| 3 | Enabling / Other | De-Scoped: Stand-alone LD provides Responder CI to one or more VRS Providers |
| 4 | Requesting | Initiation of a Verification Request (VR) via Requestor using their own internal system interfaced to the Requestor's VRS or Requestor using their VRS Provider's system. |
| 5 | Requesting | Routing of a VR between two VRS Providers. This interaction is invoked when the Responder elects to interact with a single VRS Provider which is different than the VRS Provider of the Requestor. Note: This step is not needed if the request and response are within one solution provider (one VRS). |
| 6 | Requesting | Delivery of a VR from a VRS to a Responder. |
| 7 | Responding | The reply to VRs from the Responder indicating whether the PI provided in the VR are valid. |
| 8 | Responding | Routing of the Response to a VR between two VRSs. This interaction is invoked when the Responder elects to interact with a single VRS Provider which is different than the VRS Provider of the Requestor.. Note: This step is not needed if the request and response are within one solution provider (one VRS). |
| 9 | Responding | Delivery of the Response to a VR from the Requestor's VRS to the Requestor. |

3.3 Solution Architecture Illustrations

The following illustrations depict the VRS Solution Architecture variations:

Illustration 3.3.1: VRs are routed within a blockchain and between blockchain / non-blockchain systems

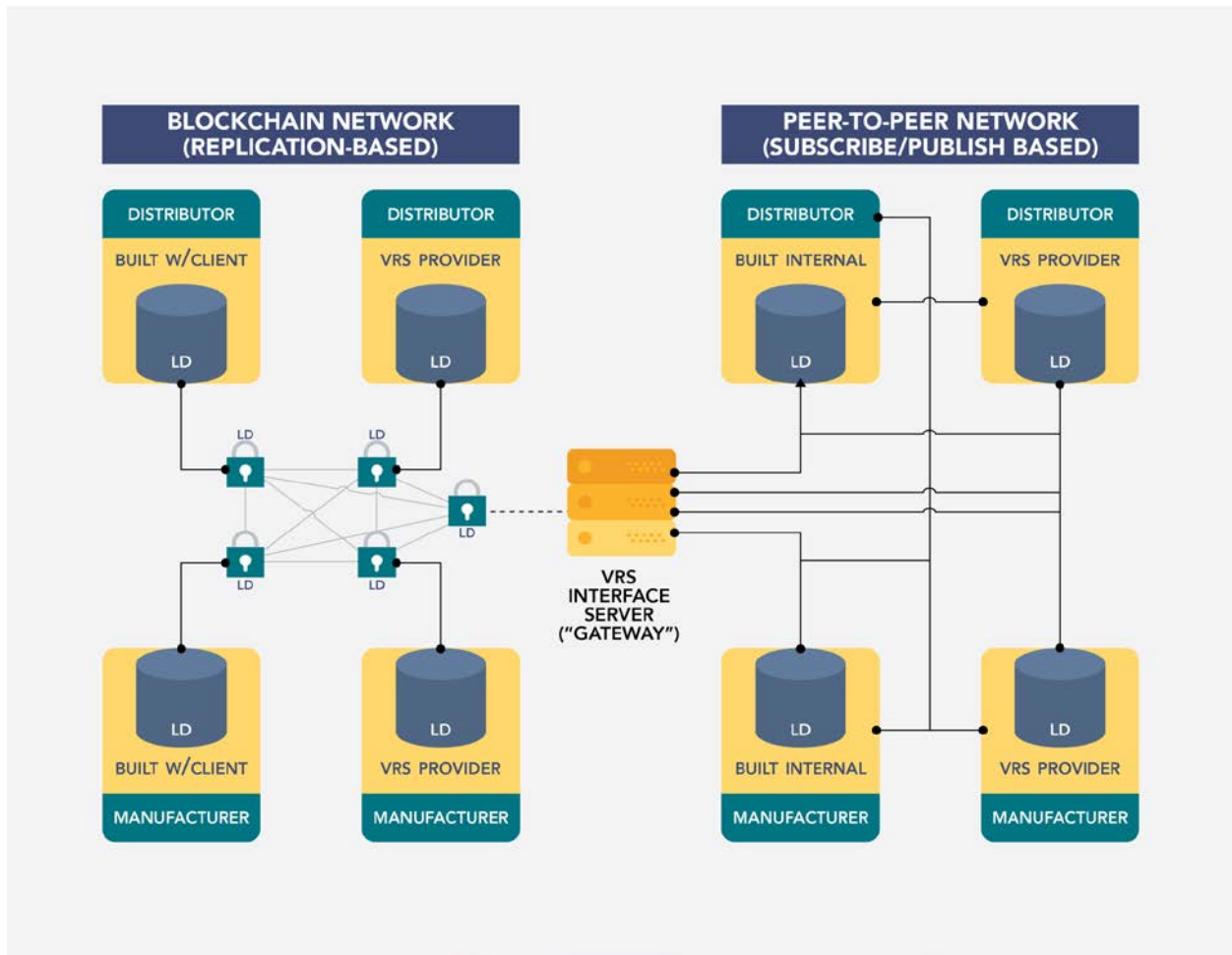
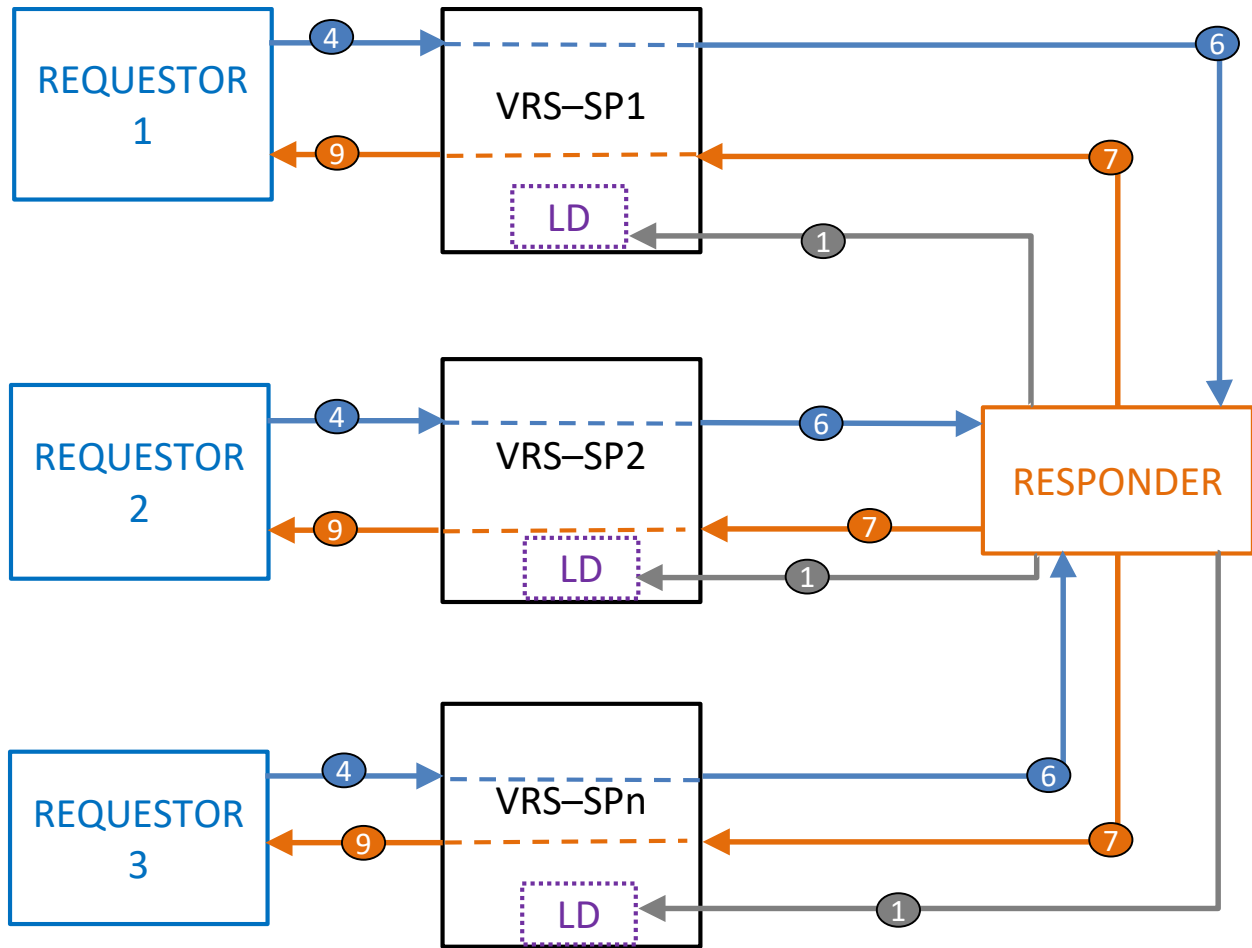


Illustration 3.3.2: VRs routed through the VRS Provider of the Requestor



In this scenario the Responder provides their Connectivity Information (CI) directly to each VRS solution provider as part of the Responder's on-boarding / security access procedure. Interaction #2 is therefore not in scope for this scenario. This scenario has also been referred to as the "Responder Build It Yourself" model as the Responder will manage their own solution for issuing responses to verification requests from entities for which the Responder also manages access.

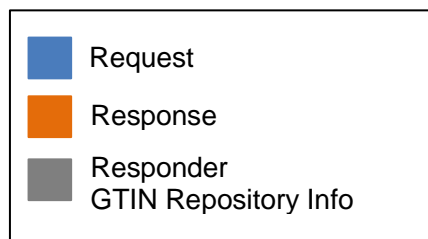
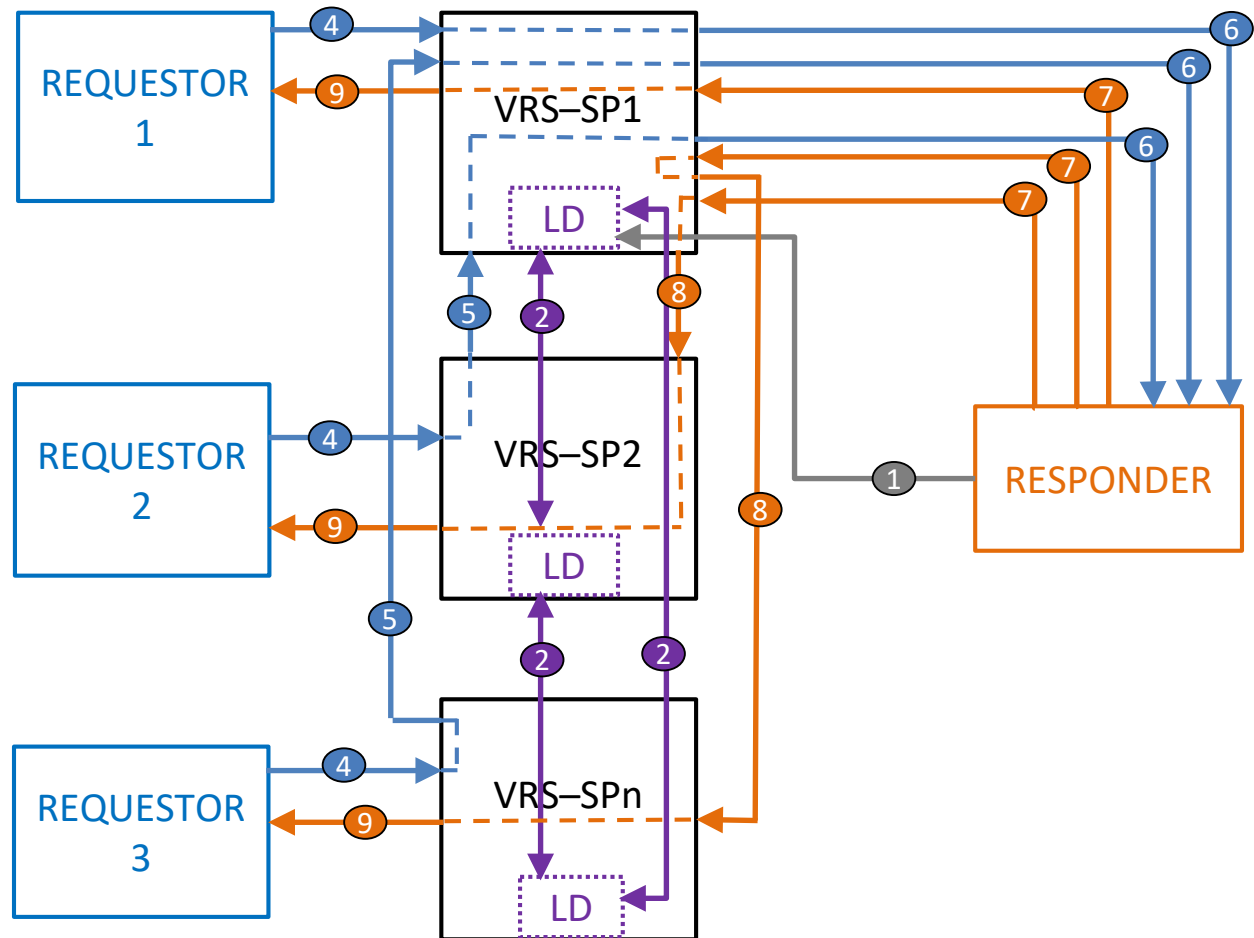
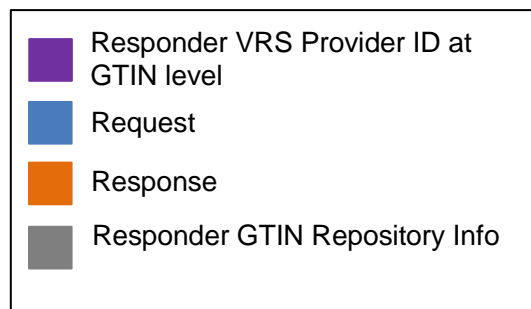


Illustration 3.3.3: VRs routed through the Responder's VRS Provider



In this scenario the Responder's VRS solution provider Connectivity Information is shared across VRS providers. Interaction #1 is therefore between the Responder and their selected VRS Provider.



3.4 Communications Protocol & Data Elements for Interactions

3.4.1 Interaction 1:

Connectivity Information (CI) at GTIN level provided by the Responder to a VRS Provider's LD.

Refer to the *VRS LD Spec* document for field-level definitions/validations and additional technical information.

3.4.2 Interaction 2:

The exchange of LD amongst VRS Providers.

Refer to the *VRS LD Spec* document for field-level definitions/validations and additional technical information.

3.4.3 Interaction 4:

Initiation of a Verification Request (VR) via Requestor using their own internal system interfaced to the Requestor's VRS or Requestor using their VRS Provider's system.

Refer to the *GS1 Verification Messaging Standard* document for field-level definitions/validations and additional technical information.

3.4.4 Interaction 5:

The routing of a VR between two VRS providers. This interaction is invoked when the Responder elects to interact with a single VRS Provider which is different than the VRS Provider of the Requestor.

Refer to the *GS1 Verification Messaging Standard* document for field-level definitions/validations and additional technical information.

3.4.5 Interaction 6:

The delivery of a VR from a VRS to a Responder.

Refer to the *GS1 Verification Messaging Standard* document for field-level definitions/validations and additional technical information.

3.4.6 Interaction 7:

Responder provides reply to VRS indicating whether the PI provided in the VR are verified, including ability to provide optional information.

Refer to the *GS1 Verification Messaging Standard* document for field-level definitions/validations and additional technical information.

3.4.7 Interaction 8:

The routing of the Response to a VR between two VRSs. This interaction is invoked when the Responder elects to interact with a single VRS Provider which is different than the VRS Provider of the Requestor.

Refer to the *GS1 Verification Messaging Standard* document for field-level definitions/validations and additional technical information.

3.4.8 Interaction 9:

The delivery of the Response to a VR from the Requestor's VRS to the Requestor.

Refer to the *GS1 Verification Messaging Standard* document for field-level definitions/validations and additional technical information.

Appendix

4.0 Assumptions

1. Multiple VRS Solution Providers will exist and each VRS will contain a Look-Up Directory (LD) as an integrated component.
2. VRS Solution Provider systems may utilize blockchain (distributed, replicated ledger); conventional, peer-to-peer transmittal of data; or both.
3. VRS solutions must minimally provide Electronic Record capabilities in order to have an audit trail of changes to master data, configuration data, and transactional data.
4. A registry comprised VRS_Provider_IDs and associated name/contact information will be maintained.
5. Exception processing across Requestor, Responder, and VRS Provider systems for missing/incomplete master data or transactional data elements, including but not limited to Responder Connectivity Information (CI), GTIN Look-Up Directory (LD) information, and Product Identifier (PI) information, will be documented by Solution Providers as part of system design activities.
6. A Responder may choose to build and/or manage their PI Repository and verification responses and will need to provide their CI either to a solution provider (for replication to all other LDs) or provide their CI directly to distributors for whom they want to provide responses for verification requests. A Requestor may also build their own requesting services and will make necessary connections and updates to be a member of the VRS network.