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

Chapter 5: Tracing Architecture Functional Design

Version 1.6
July 15, 2026

Table of Contents

Table of Figures

Chapter 5: Tracing Architectural Functional Design

Introduction

Why traces are initiated? Product ownership traces are executed to support suspect, illegitimate, or recalled product investigations or for compliance audits.[1] Traces gather information about products, supply chain partners, and exchange of ownership. Tracing within the PDG-defined EDDS network has been limited to these investigation types to mitigate against gathering product, company, and supply chain information for nefarious or business intelligence purposes.

Within the PDG-defined EDDS network, traces are executed as a series of TI requests and TI responses initiated by the investigating party until that party has satisfied their investigation needs. Within the PDG-defined EDDS network, a trace requester may be a DSCSA-defined authorized trading partner (ATP[2]), industry-recognized trading partner (ATP equivalent[3]) or an industry-recognized DSCSA Authority.[4] There are many aspects to investigations driven by regulatory, legal, and business policy. A TI Request results in information gathered to help in the investigation. By its very nature, it also provides the Responder with some documented information about the investigation itself.

Secure exchange interface methods (ex: OpenAPI[5] or DIDComm[6]), the proper use of credentials and structured JSON messages conformant to the TI Request or TI Response schemas in the Appendix, represent the most technically secure, verifiable and trustworthy method of executing trace interactions. This chapter provides TI Request and TI Response message designs, proposed JSON schemas and credential usage that incorporate data element formatting, cardinality and mandatory/optional/contextual requirements developed in the PDG design process. It is expected that trading partners and solution providers will test, pilot, standardize and implement these methods, credentials and messages to accommodate trading partners within a full range of technical capabilities and constraints in support of early adoption and technical maturity as experience with tracing progresses. The *Recommendations* section provides insight into how this technical maturity might transition into a secure, interoperable distributed network.

Purpose of the Document

Chapter 1 provides requirements and recommendations supporting interoperable tracing for the purposes of:

1. Investigating a suspect product.
2. Investigating an illegitimate product.
3. Investigating recalled product.
4. Demonstrating tracing capability as part of a compliance audit.

This chapter provides functional design and requirements to be implemented by trading partners, authorities and trace solutions to trace product using the PDG-defined DSCSA EDDS network in support of suspect product, illegitimate product, recalled product investigations and compliance audits.

---

[1] For the purposes of this document, Compliance Audits are considered a type of investigation.
[2] ATPs must prove their identity and that they have an appropriate Federal or State registration or license. See Chapter 6 – Credentialing for further information.
[3] ATP equivalents are organizations that are not required to hold ATP qualifying registrations or licenses but are trading partners that must comply with the DSCSA. See Chapter 6 – Credentialing for further information.
[4] DSCSA Authorities are authorities referenced in the DSCSA statute. See Chapter 6 – Credentialing for further information.
[5] OpenAPI Specification is an open-source format and initiative for designing and creating machine-readable interface files that are utilized in producing, describing, consuming, and visualizing RESTful APIs and web services.
[6] DIDComm, short for Decentralized Identifier Communication, is a communications methodology that works with the decentralized design of DIDs to provide private, secure interaction.

The Tracing Functional Design provides detailed information on *how* DSCSA Transaction Information and Transaction Statement information (TI and TS data) is gathered to form a trace of drug product ownership going back to the Manufacturer or Repackager in support of suspect, illegitimate and recalled product investigations utilizing the PDG-defined EDDS network.

This document is created based on the high-level requirements for interoperable tracing (Chapter 1) and functional requirements, constraints, and architectural design of the PDG Tracing Architectures Work Group and agreed to by PDG membership. Included in this section are detailed functional requirements including use cases, system inputs and outputs, process flows, diagrams, and sample tracing scenarios.

Tracing Model

In the DSCSA context, tracing is the act of gathering the full set of TI and TS data available from trading partners such that the ownership history is established for the package or case in question. In practice, tracing a package or case is executed in a series of TI Requests and TI Responses upstream and/or downstream from the trading partner initiating the requests (or by a regulatory authority). By this process, the Requester acquires TI and TS datasets until the entire ownership chain is documented. *Figure 1* depicts the PDG-defined tracing model for all parties that seek to utilize the PDG-defined EDDS network. Upon receiving a trace request, trading partners (with the help of their solutions) provide the TI and TS data they received from their suppliers as well as TI and TS data they sent to their customers. The TI and TS data can either be sourced from the trading partner's TI and TS repository or accessed from TI and TS repository maintained by their seller.

The PDG-defined tracing functionality allows for flexibility for trading partners involved in suspect, illegitimate or recalled product investigations. Requesting trading partners or authorities can execute as many TI Requests as needed to support their investigation (a full end-to-end trace is not mandatory). In addition, Requesters may also specify one of three data set types to be returned in the trace response:

- **TI and TS:** the Responder returns all TI and TS datasets they have either received or sent.
- **All known owners:** the Responder returns information on all known owners they have information for (typically, who they purchased from, themselves and who they sold to).
- **Last known owner:** the Responder returns information on the last known owner they have TI for (typically, themselves or who they sold or returned the product to).

It is expected that TI Requests may result in the Responder wanting to contact the Requester to either resolve an exception or to gain clarity on the Request. Likewise, Requesters may want to contact the Responder for clarity on the response received. To support these communications, each TI Request and TI Response includes contact information of the Requester or Responder.

Each TI Response (see *Appendix 2 – TI Response JSON Schema*) data set also returns the trace endpoint for each trading partner involved in the TI and TS exchange, allowing the Requester to continue their TI Requests up or down the ownership chain.

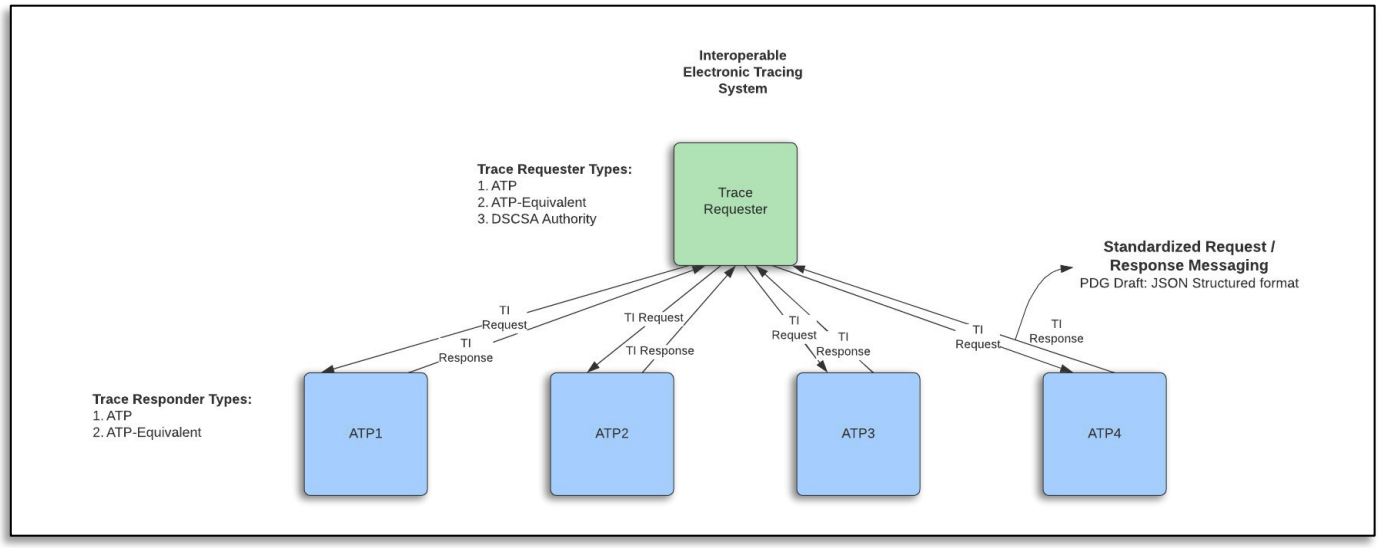

Figure 1 - PDG-Defined EDDS Tracing

Tracing Model Components

The processing steps in this section are illustrative to give a sense of what the component does. The actual order of steps will be determined by the Tracing and Digital Wallet solutions.

Trace Requester System

The Requester's system is used for the following processes required to submit a TI Request and receive a TI Response:

- Create TI Request message (allow for a Trace Requester to create TI Request in the Trace Request System).
- Request Requester's digital credential (ATP, ATP-Equivalent or DSCSA Authority) from the Digital Wallet.
- Submit TI Request message.
- Receive TI Response(s).
- Process TI Response.
    - Authenticate and Authorize Trace Responder.
        - Request Digital Wallet verify credential[7]; or
        - Perform Responder DSCSA authenticity[8] and authority[9] checks.
    - Check TI Response(s).
    - Transaction logging.

Trace Responder System

The Responder's system is used for the following processes required to receive a TI Request and submit a TI Response:

- Receive TI Request.

[7] See OCI Digital Wallet OpenAPI specifications.
[8] Determine the identity of the Responder.
[9] Determine if the Responder is an Authorized Trading Partner (ATP), or an ATP Equivalent.

- Authenticate and Authorize Trace Requester.
  - Verify credentials (see Digital Wallet); or
  - Perform Requester DSCSA authenticity[10] and authority[11] checks
- Check TI Request Message.
- Process TI Request Message.
  - Create TI Response Message.
  - Present TI Request and available TI Response information for Trace Responder review
  - Request TI Responder ATP, ATP-Equivalent credential presentation from Digital Wallet. Submit TI Response message.
  - Transaction logging.

Digital Wallet

Digital wallets of the TI Requester or TI Responder are invoked by the TI Requester or TI Responder solution system to provide:

- Authenticate access to Digital Wallet
- Generate ATP, ATP-Equivalent or DSCSA Authority verifiable credential in JWT presentation for use in TI Requests and TI Responses
- Check the received JWT presentation of the ATP, ATP-Equivalent or DSCSA Authority verifiable credential

Trace Messages

Traces are accomplished through a series of interoperable TI Requests and TI Responses. Each set of Requests and Responses provide information on the ownership of the product and provide the endpoint where the Requester can continue their product ownership trace with the previous or next owner of the product.

TI Request Message

Provides interoperable information about the Requester, the products they are seeking to trace, the circumstance of the investigation being prosecuted, and the kind of information requested to be returned.

TI Response Message

Provides interoperable information about the Responder, the products that the Requester is tracing, the kind of information requested to be returned and trace endpoints associated with known buyers and sellers for the Requester to use in continuing their trace.

Trace Endpoints

Each trading partner (ATP and ATP-Equivalent) shall exchange their preferred trace method and trace endpoint where TI Request messages can be submitted. Initially during the proof-of-concept or proof-of-technology phase(s)[12], it is thought that email addresses will be used as trace endpoints to exchange standardized TI Request and TI Response messages. As the trace eco-system enters the production phase[13] the PDG-defined EDDS network will move to OpenAPI or DIDComm to exchange messages securely and privately.

[10] Determine the identity of the Requester.
[11] Determine if the Trace Requester is an Authorized Trading Partner (ATP), an ATP Equivalent, or a DSCSA Authority.
[12] Assessment of trace volumes, trial of TI Request/Response messaging and trial of exchange mechanisms.
[13] See *Recommendations*.

DSCSA Authentication and Authorization Checking

The preferred method of checking the authenticating (determine identity) and authorizing (determine ATP, ATP-Equivalent, DSCSA Authority status) of the Requester or Responder is using W3C standard digital credentials (see Chapter 6, Credentialing) as documented by OCI open specifications[14]. During the transition to digital credentials, TI requests and TI responses may be exchanged without the proper digital credential, leaving the receiving party with the task of manually:

- authenticating the identity of the Requester or Responder who sent the message
- authorizing the requesting or responding entity by checking their ATP, ATP-Equivalent or DSCSA Authority status

Credentialing for Tracing

TI and TS Exchange takes place between established trading partner pairs in a controlled electronic environment where the "credentialing" requirement is fulfilled by existing Know Your Customer / Know Your Supplier (KYC/KYS) processes that each trading partner is responsible for. Alternately, PI Verification and Tracing is architected to occur using decentralized architecture where individual trading partners (through their systems) acquire another trading partner's digital endpoint, establish a digital connection, and authenticate each other in the digital interaction process (either PI Verification or tracing) using digital credentials or manual Authentication and Authorization processes. These interactions often occur between non-adjacent trading partners who have not performed Know your Customer / Know Your Supplier processes prior to the PI Verification or Tracing digital interactions.
The digital credential architecture adopted by PDG[15] is leveraged in TI Request/Response interactions to support an efficient, interoperable, electronic, and decentralized eco-system. Digital credentials in TI Requests or Responses provide cryptographically verifiable Identity and authority[16] information of the entity Requesting TI or Responding to TI Requests.

However, PDG recognizes that individual trading partner pairs may address "credentialing" outside the PDG-defined DSCSA EDDS network. Two are possible, however they fall outside the PDG-defined EDDS network architecture for Tracing:

> **KYC/KYS and direct connections:** Employs the same processes TI and TS exchange relies on for trading partner pairs to accomplish authentication and authorization through their existing processes for establishing a trading partner's identity and ATP status AND by establishing direct and secure connections between their systems.
>
> **Ad-Hoc credentialing process:** For an entity to respond to a PI Verification or Tracing request, they must first ascertain the requester's identity and "authorized" status. This process could be initiated using the Requester's "Contact Information". The trading partners would then perform their internal processes for establishing a trading partner's identity and ATP status. Each subsequent TI Request will trigger this same process.

Chapter 6 addresses the use of Decentralized Identity and Verifiable Credentials as the means to support the decentralized architecture and requirements for an interoperable, PDG defined EDDS network including tracing.

[14] OCI: Open Credentialing Initiative: www.oc-i.org.
[15] PDG Blueprint, Chapter 6: Credentialing and Trading Partner Authentication and Authorization.
[16] The Requester or Responder is either an ATP, ATP-Equivalent or a DSCSA Authority.

High-Level Functional Interactions

Figure 2 depicts a typical interaction between a TI Requester and TI Responder. Each ATP or ATP-Equivalent

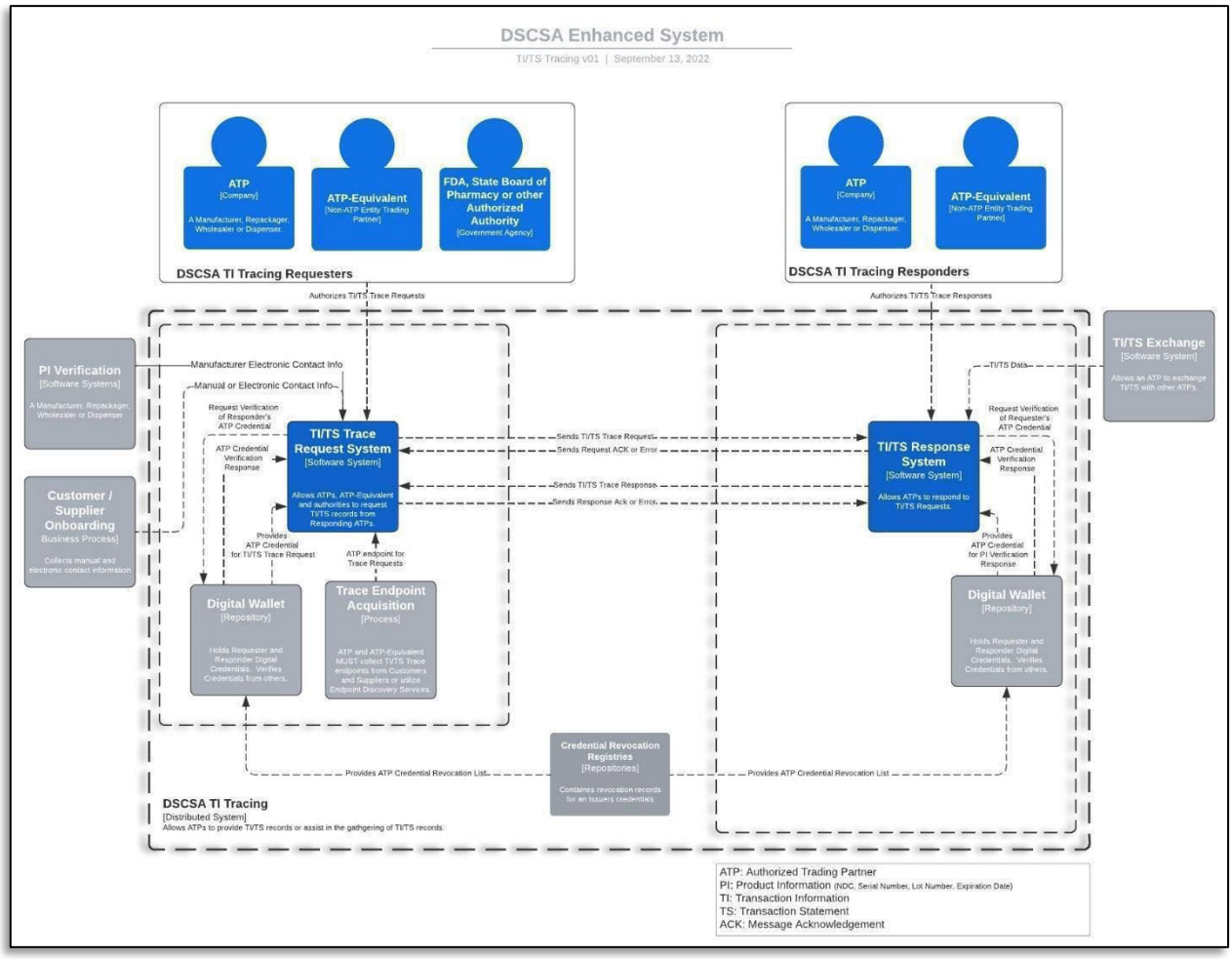

Figure 2 - TI and TS Trace Request and TI Response

Figure 3 provides an illustration of how a TI Request / TI Response exchange might take place using OpenAPI as the exchange mechanism. In this example, standard OpenAPI acknowledgement of messages received (TI Requests and TI Responses) are used.

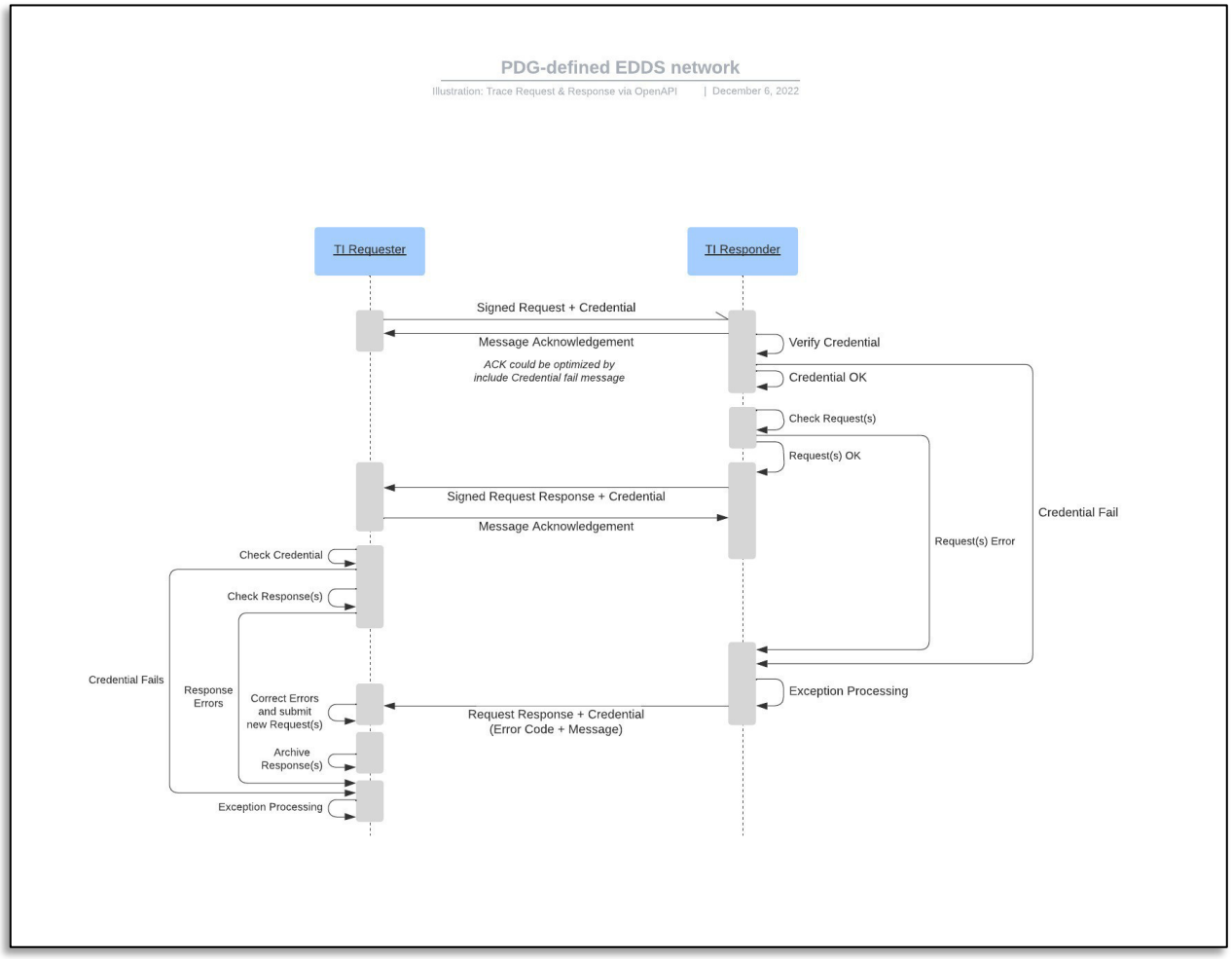

Figure 3 - Illustration of TI Request/Response choreography using OpenAPI exchange method

Figure 4 provides an illustration of how a TI Request / TI Response exchange might take place using email as the exchange mechanism. In this example, the party receiving a request or response must send an acknowledgement to the sender. This can be done manually or through application/email configuration.

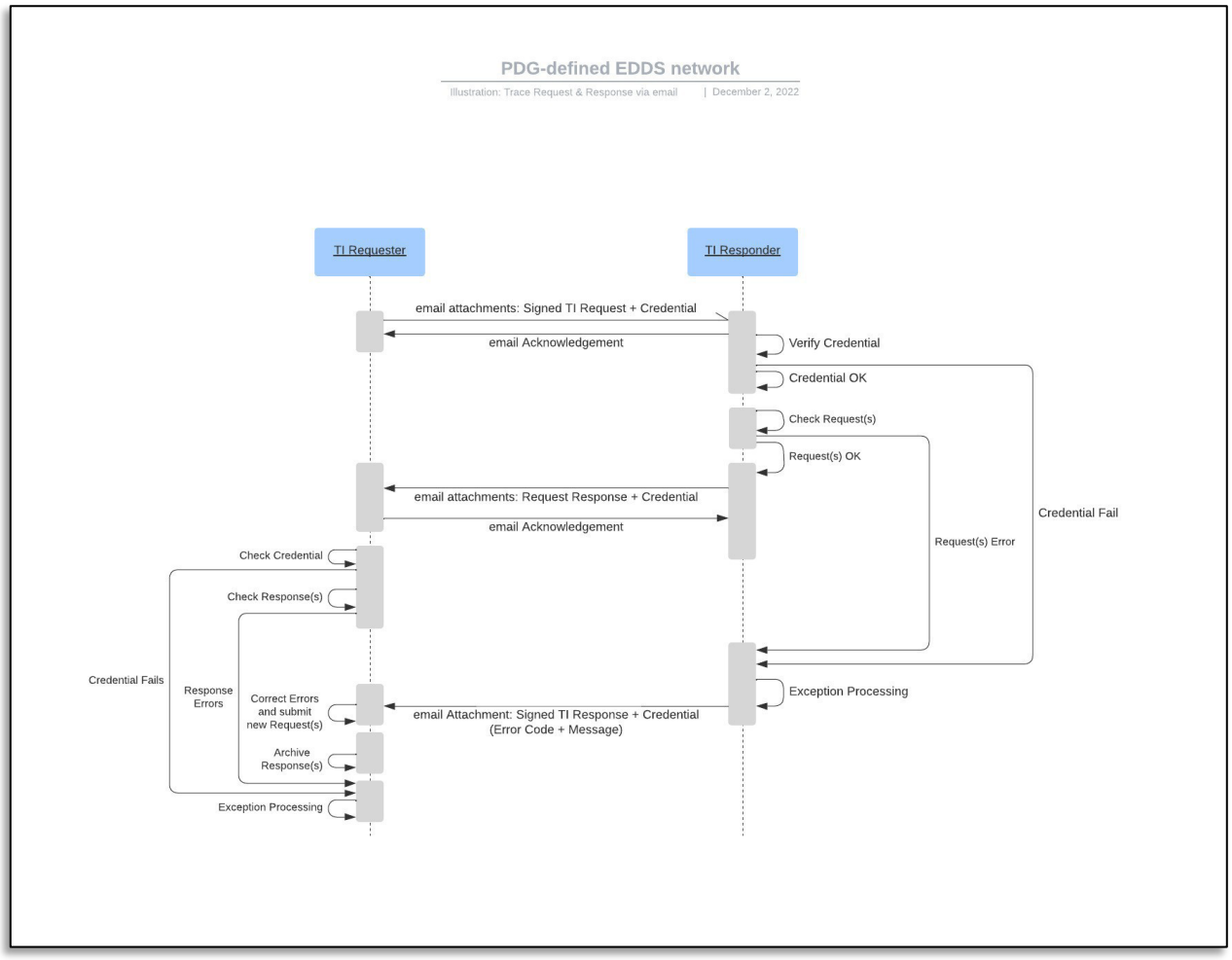

Figure 4 - Illustration of TI Request / Response choreography using email exchange method

Figure 5 provides an illustration of how a TI Request / TI Response exchange[17] (exchange method unspecified) might take place without using digital credentials as specified in this chapter and Chapter 1. It is anticipated that there will be a transition period for using credentials. As an illustration, trading partners are aware of their current onboarding processes from a timing and cost perspective that will need to be used (*Figure 5*, Manual Identity and ATP status discussion).

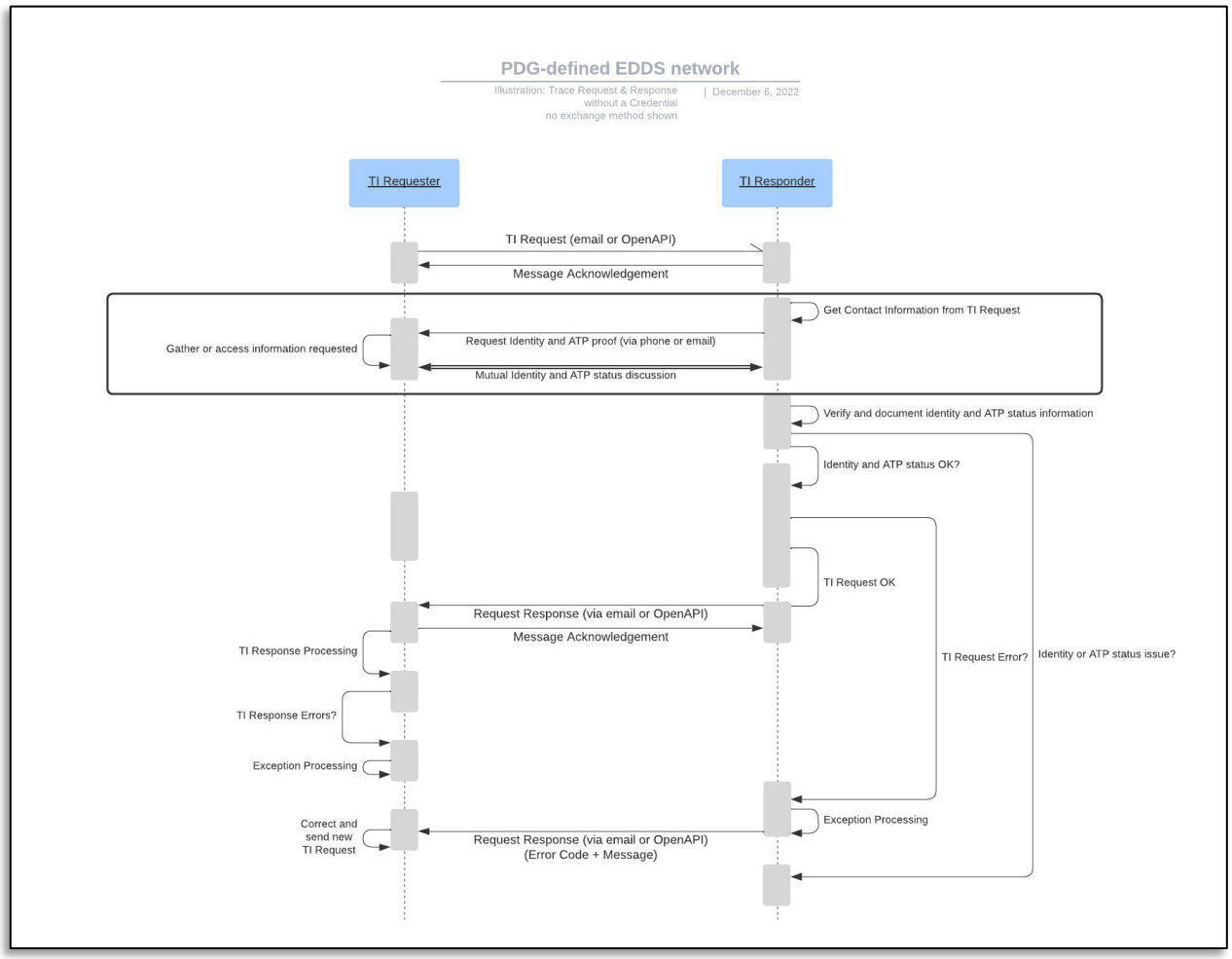

Figure 5 - Illustration of TI Request / Response choreography without credentials

[17] See *TI Request Structure and TI Response Structure*.

Exception Processing and Supplemental Messaging

Figures 4, 5, and 6 illustrate error messages provided by the Responder. Requesters can correct errors in their request and submit the corrected TI Request. If the Requester is unable to submit an acceptable Request, they can use the Contact Information provided in the TI Response Party section of the TI Response message to contact the Responder.

Supplementary messages can be provided addressing the entire Request, or for individual Requests identified by the Request Line Number. It is envisioned that standard supplementary and error messages will be developed as part of the TI Request / TI Response standardization process. The following messages are illustrative and are applied at the Request set and individual Request levels.

Messages Applied at the Entire Request Level (Illustrative)

These supplemental or exception messages apply to the entire Request message identified by the TI Request ID.

Code	Message	Type	Meaning
RM-001	Credential verification failed	Exception	Checks of the ATP Credential provided failed.
RM-002	Request parameter error	Exception	Required parameter not provided, or invalid combination of parameters provided (ex: non-authority attempting a lot-level request).
RM-003	Compliance audit Request received	Supplemental	The Responder acknowledges the Requester's Investigation Reason Attestation. No TI or ownership data is provided.
RM-004	Request model verification failed	Exception	The TI Request message format does not match the published model.

Messages applied at the Request Line Level (Illustrative)

These supplemental or exception messages apply to an individual Request within the Request message identified by the Request Line Number.

Code	Message	Type	Meaning
RL-001	Request Closed	Supplemental	Indicates that there will be no further action on the Responder's part and the Responder considers the Request closed.
RL-002	No TI found for the Request	Supplemental	The Responder does not have any TI or Ownership info matching the individual Request.
RL-003	Response Delayed	Supplemental	The Responder is researching the Request and will respond at a later time.
RL-004	Request addressed via your supplied Contact Information	Supplemental	The Responder has contacted the Requester and addressing the Request outside of this channel.
RL-005	Request GTIN, NDC, Lot Number or Serial Number not formatted correctly.	Exception	One or more of the key attributes provided in the Request are not formatted correctly.
RL-006	Response includes an Intracompany Transfer.	Supplemental	Requester's Transfer-To party of their inbound TI and Requester's Transfer-From party of their outbound TI may not match as a result of an intracompany transfer.

Tracing and Records Retention

Trading partners are required to keep records of Suspect and Illegitimate product investigations for six (6) years after the investigation. Your company's compliance policy may require TI and TS datasets acquired through the tracing process be retained as part of the investigation documentation set archived.

Connectivity Requests

It is envisioned that when OpenAPI or DIDComm are used to exchange messages securely and privately, provisions are made to test for connectivity to another party's system in the network.

Trace Messages

As a Requester, an ATP, Authority, or ATP-Equivalent organization may request TI for an individual or multiple pharmaceutical package or case.

TI Request Message Structure

Figure 6 illustrates the high-level organization of a TI Request message, designed to provide a responding organization with:

- **Audit references** including TI Request ID and Request Timestamp
- **Requesting Party Information,** providing the Responder with a verifiable credential, contact information and electronic callback information
- **Request Parameters,** including information about the related investigation, the kind of information being requested, and other information related to the request
- **Individual Requests,** indicating the individual GTIN or NDC and Serial Number or Lot Number (only for DSCSA Authority requests for recalled product).

This provides the responding organization everything they need to understand the circumstances of the request, research their records, review both the request and assemble response(s) and respond to the Requester. *Figure 7* illustrates the detailed organization of the TI Request message.

As TI Requests are only allowed for the purposes of Suspect, Illegitimate, or Recalled products, or for the purposes of a compliance audit, TI Request and TI Response records should be retained as part of those investigation records.

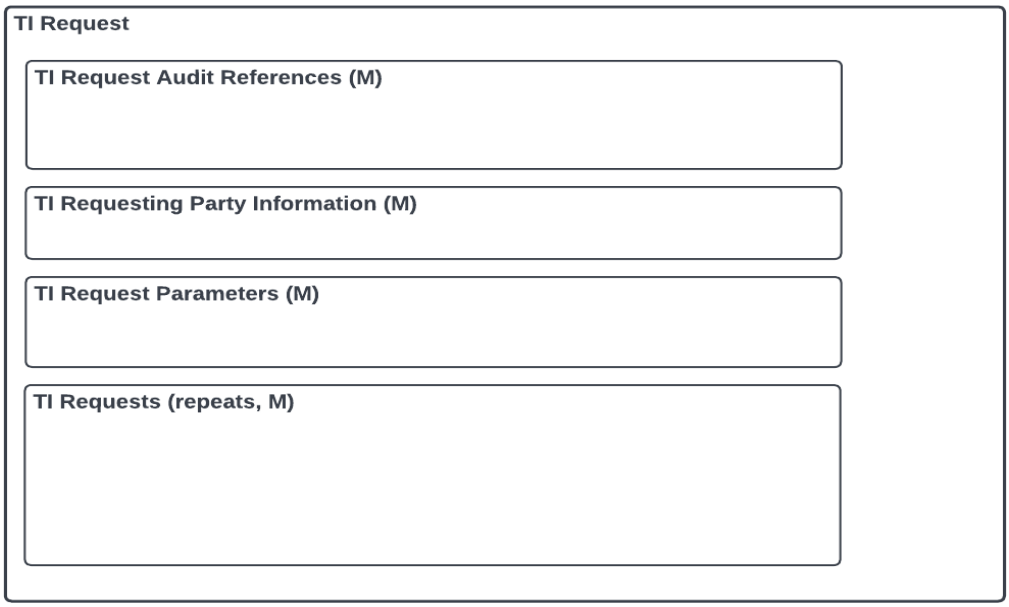

Figure 6 - High-Level TI Request Message Structure

TI Response Message Structure

Figure 8 illustrates a high-level view if the TI Response message, designed to provide a requesting organization with:

- **Audit references** including TI Request ID, TI Response ID and Response Timestamp
- **Responding party Information,** providing the Requester with a verifiable credential and contact information.
- **Request Responses,** providing Transaction Information or Organizational Information based on the Requester's Response Type Requested
- **Response Message,** is provided in place of Transactional or Organizational information if there are exceptions that address the entire Request set.

As multiple items can be requested in a TI Request message, the Response message provides Audit and Responding party information as well as responses to each individual request line number. In addition, a message can be provided in the "Response Message" in response to the entire request set. It is envisioned that this is where exception processing messages to address Request parameter errors, ATP Credential verification failure and other exceptions at the request set level. *Figure 9* illustrates the detailed organization of the TI Request message.

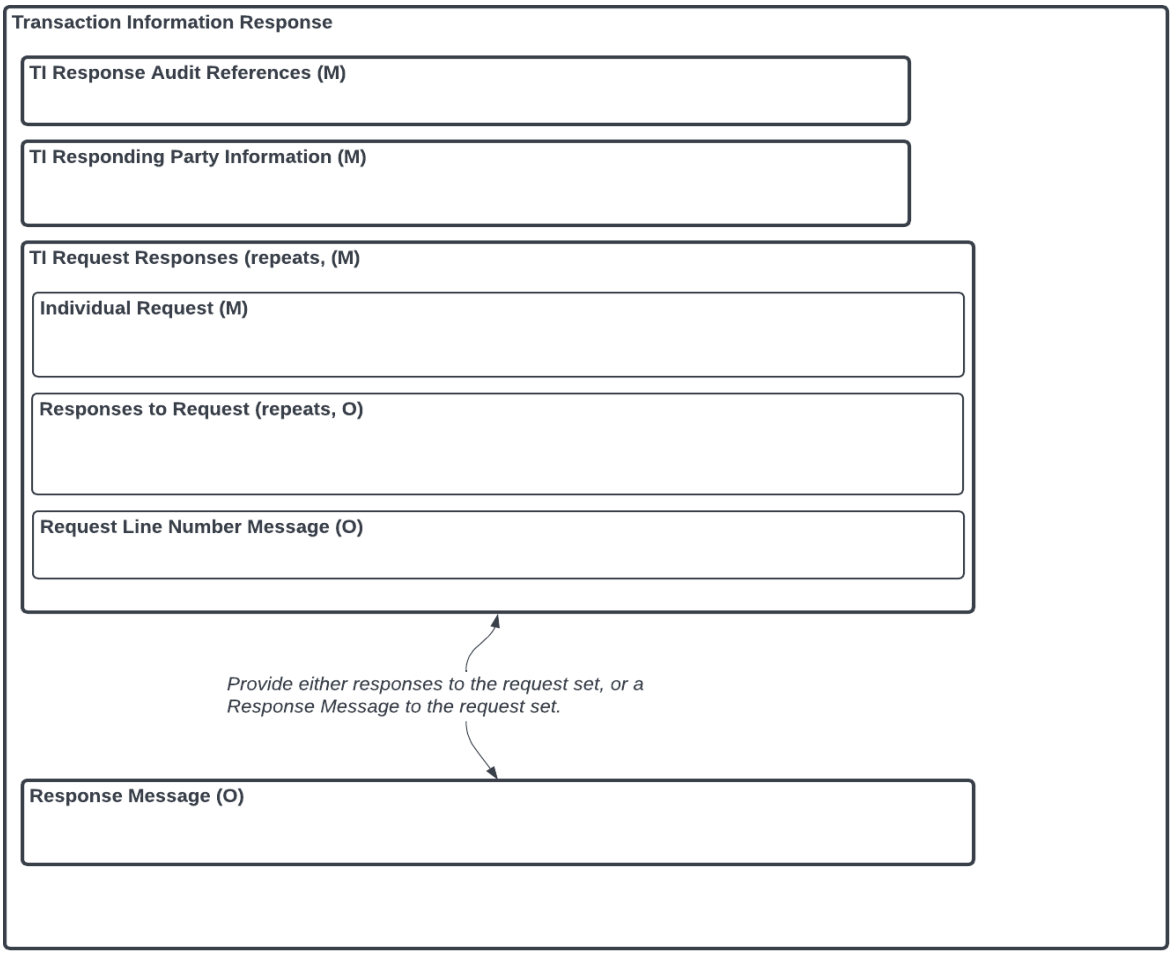

Figure 8 - TI Response Message Design - High-Level

To maintain interoperability at the data element level, the JSON Schemas, Excel Templates, and PDF Templates contain the same data structures and attributes found in the message models (TI Request and TI Response). Trade Partners, Authorities, and Solutions are anticipated to implement the rendering type that suits their needs. For model and rendered type details, see the TI Request and TI Response documentation for the model, JSON Schema, Excel Template, or PDF Template.

JSON Schemas

"JSON is an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and arrays. It is a common data format with diverse uses in electronic data interchange, including that of web applications with servers."[18]

As a proof of concept and recommended start towards standardization, the TI Request and TI Response messages are rendered in JSON format to aid in standardizing attribute definitions, constraints, and attribute format. A TI Request JSON schema and a TI Response JSON schema is provided for individual Trace solutions to uniformly validate TI Request and TI Response JSON files. An example message in JSON that validates against the schema is also provided here.

For the purposes of this document, the JSON designs are meant to allow room for the use of email, OpenAPI and DIDComm. The next phase (Piloting) will require technical work to modify the current design for use with specific exchange methods. For example, the credential is optional in the current design, which gives the opportunity to test providing a credential in the TI Request or TI Response JSON or in addition to (along with) The TI Requestor TI Response JSON (may accommodate low capability email solutions). Also, the exact rendering (JWT, JWS, etc.) of the credential may be different to fit best with the specific exchange method (email, OpenAPI or DIDComm).

Excel and PDF Templates

The JSON Excel and PDF Templates allow trade partners, authorities, and solutions to use a templated version of the TI Request and TI Response message data elements defined in the model.

[18] https://en.wikipedia.org/wiki/JSON.

Partnership for DSCSA Governance

TI Request / TI Response Messages - Data Attributes

The PDG DSCSA TI Request Model Documentation and PDG DSCSA TI Response Model Documentation contains data attribute definitions for the TI Request and TI Response messages respectively. PDG also provides detailed documentation for the JSON Schemas and user guidelines for the Excel and PDF Templates.

Tracing Choreographies[19]

Figure 10 depicts the interaction between requesters and responders at a high level. These technical interactions are accomplished through the Requester's and Responder's Trace systems or solutions.

Figure 11 introduces a sampling of processes a Responder may employ in evaluating the Requester, the Request and the TI and TS data sets that have been identified as matching the Request.

Envisioning a fuller technical set of interactions, *Figure 12* illustrates interactions between Trading partners (Requesters and Responders), their Trace solutions and their Digital Wallet solutions.

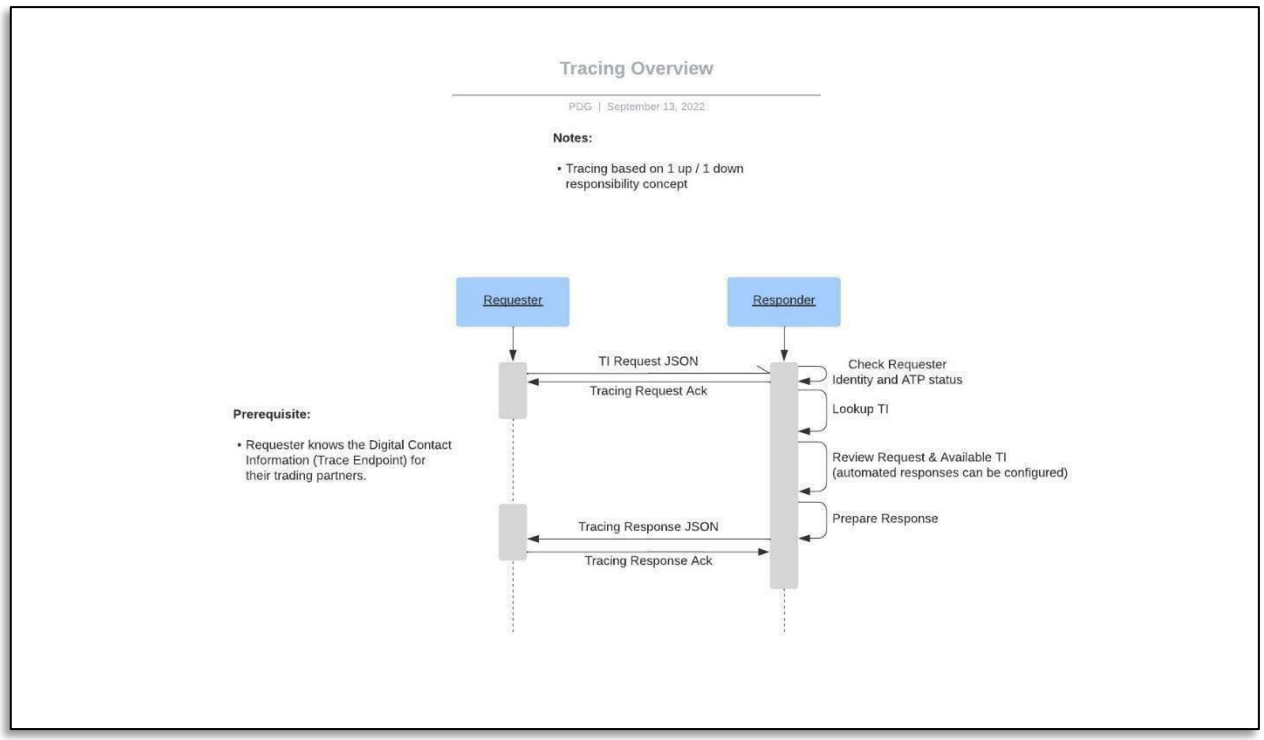

Figure 10 - High-Level Tracing Choreography

[19] These choreographies and illustrative. All internal processing steps are non-normative and are provided to illustrate how a party might process data received.

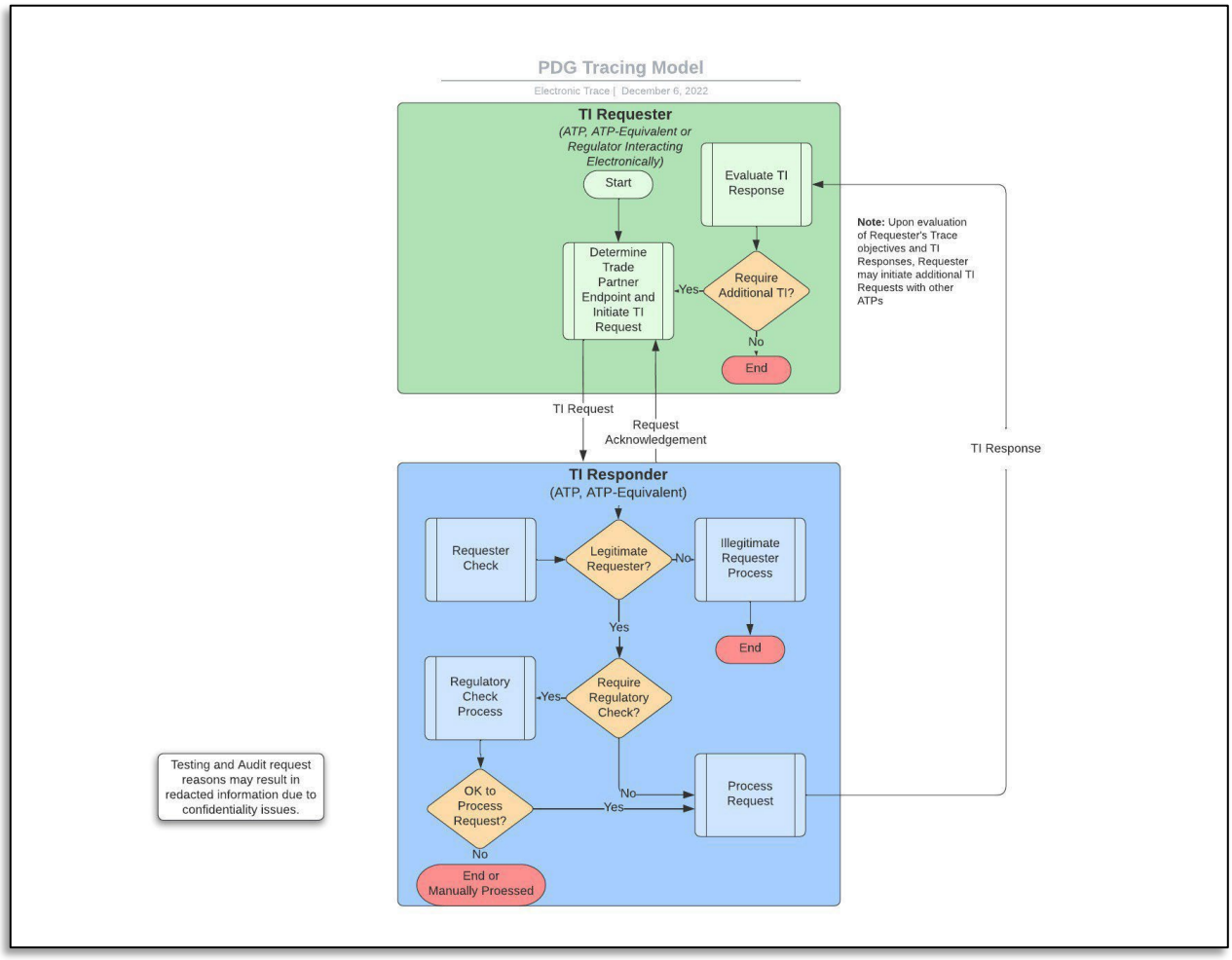

Figure 11 - Illustration: High-Level interaction and decisions of TI Requesters and Responders

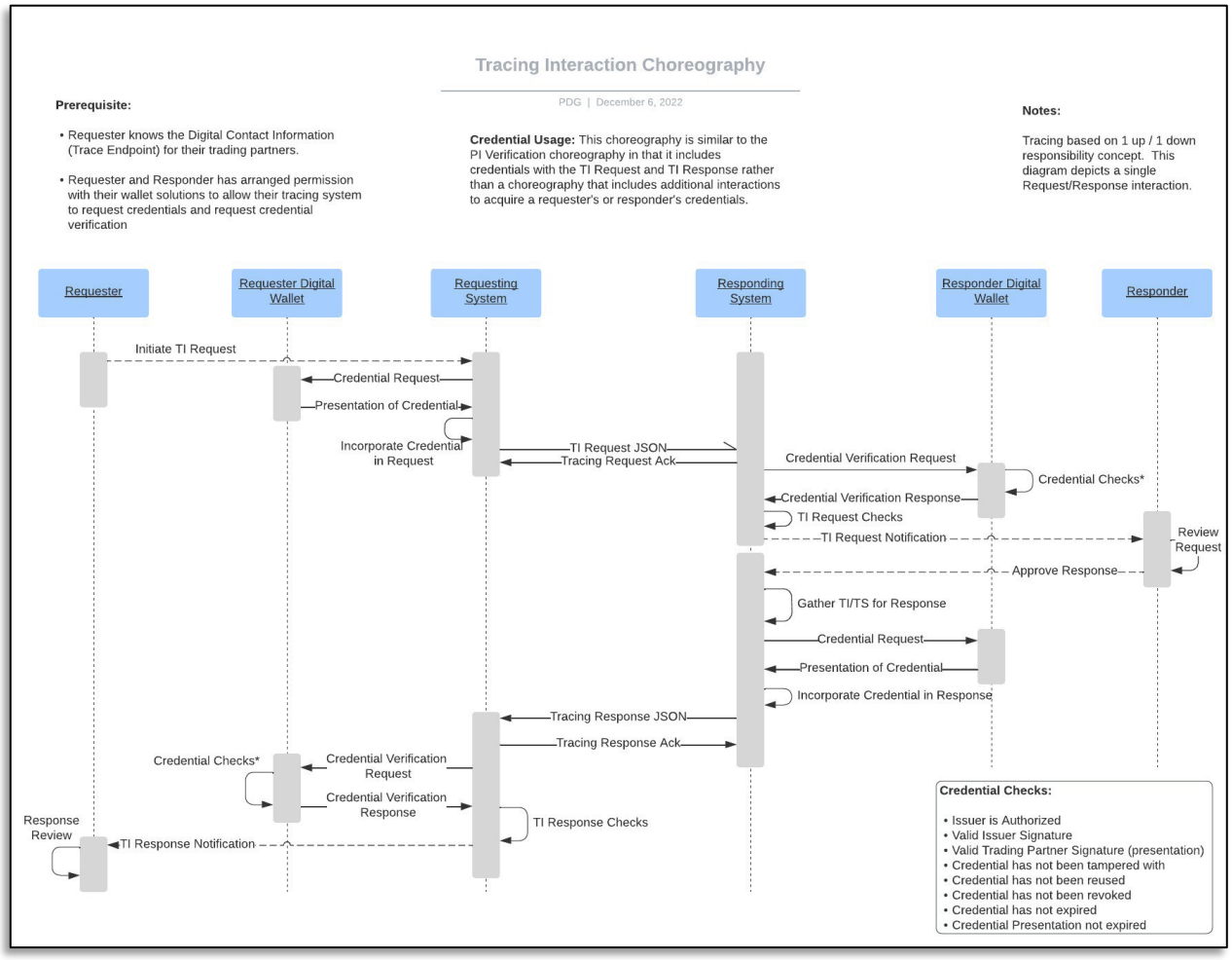

Figure 12 - TI Request / Response End-to-End Interaction

DSCSA Authorities Not Participating in the PDG-defined EDDS Network

PDG encourages DSCSA Authorities to participate in the PDG-defined EDDS Network by being credentialed as a DSCSA Authority, and by acquiring the capability of transacting TI Requests and receiving TI Responses in the form of the TI Request[20] / TI Response[21] electronic messages. However, it is recognized that not all DSCSA authorities will have the capability to participate in the PDG-defined EDDS network. In these instances, it is recommended that trading partners use elements of the PDG-defined EDDS network architecture as much as possible in responding to requests outside of the network. For example, the data attributes defined in the TI response JSON structures should be used and if the authority

[20] *Appendix 1 – TI Request JSON Schema.*
[21] *Appendix 2 – TI Response JSON Schema.*

may have some capability to use the TI response JSON format. *Figure 13* depicts how a trading partner might interact with a DSCSA Authority outside of the PDG-defined network.

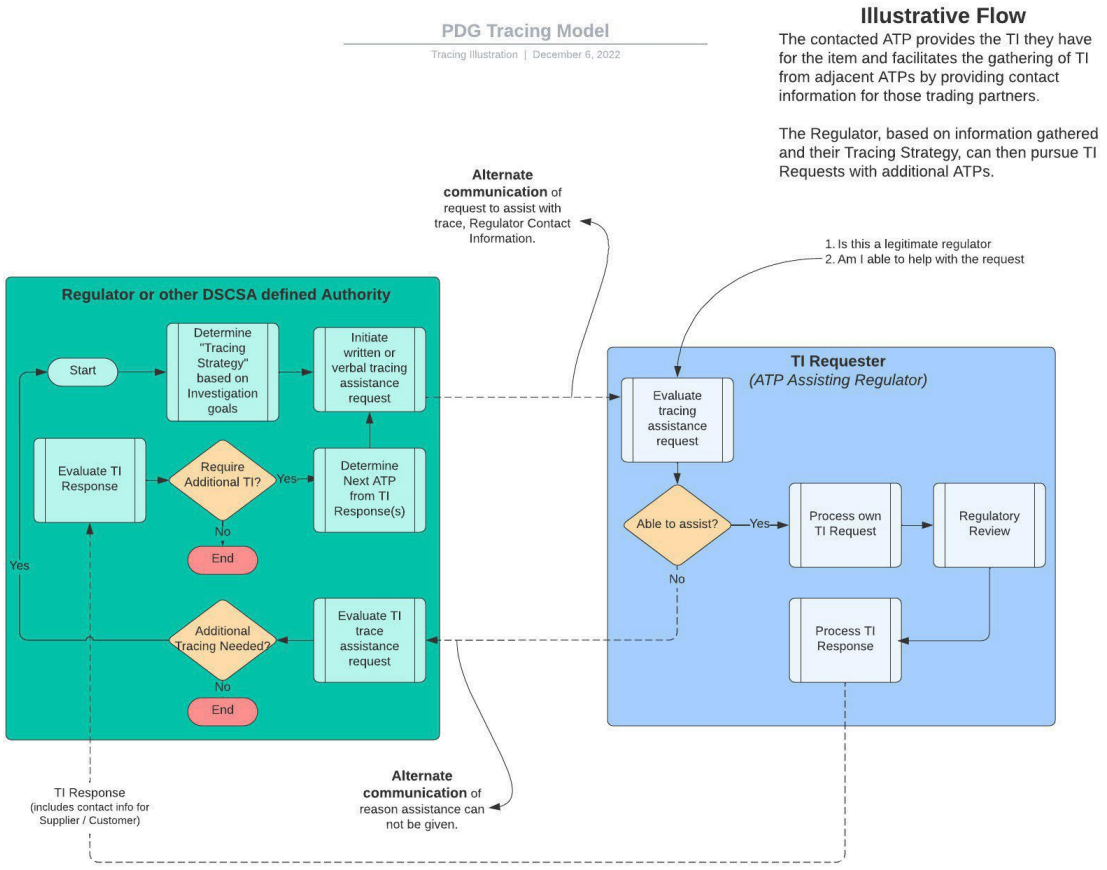

Figure 13 - Assisting a Regulator outside of the PDG-defined EDDS network

Trace Endpoint Acquisition

To utilize the trace functionality of the PDG-defined EDDS network, a trading partner (or trading partner designated system) must first acquire Trace Endpoint information for companies they have exchanged (sent and/or received) TI and TS information with.

A prerequisite to initiating a trace via a TI Request is to establish the trace endpoint where the electronic TI Request is to be sent. Solutions to discovering trace endpoints, such as resolvers, routers, look up directories, etc., have been proposed (see *Figure 14*) and will most likely be explored during the next phase of development (Proof of Technology, Proof of Concept or Pilot projects). To provide a baseline solution that allows trading partners to get started, PDG has established the process of Trace Endpoint Acquisition as part of the existing trading partner onboarding. During that process, trading partners share several technical and business information to electronically exchange TI and TS information. The requirement to also exchange each other's Trace Endpoints may not be the most sophisticated architecture, but it does allow for early tracing to take place.

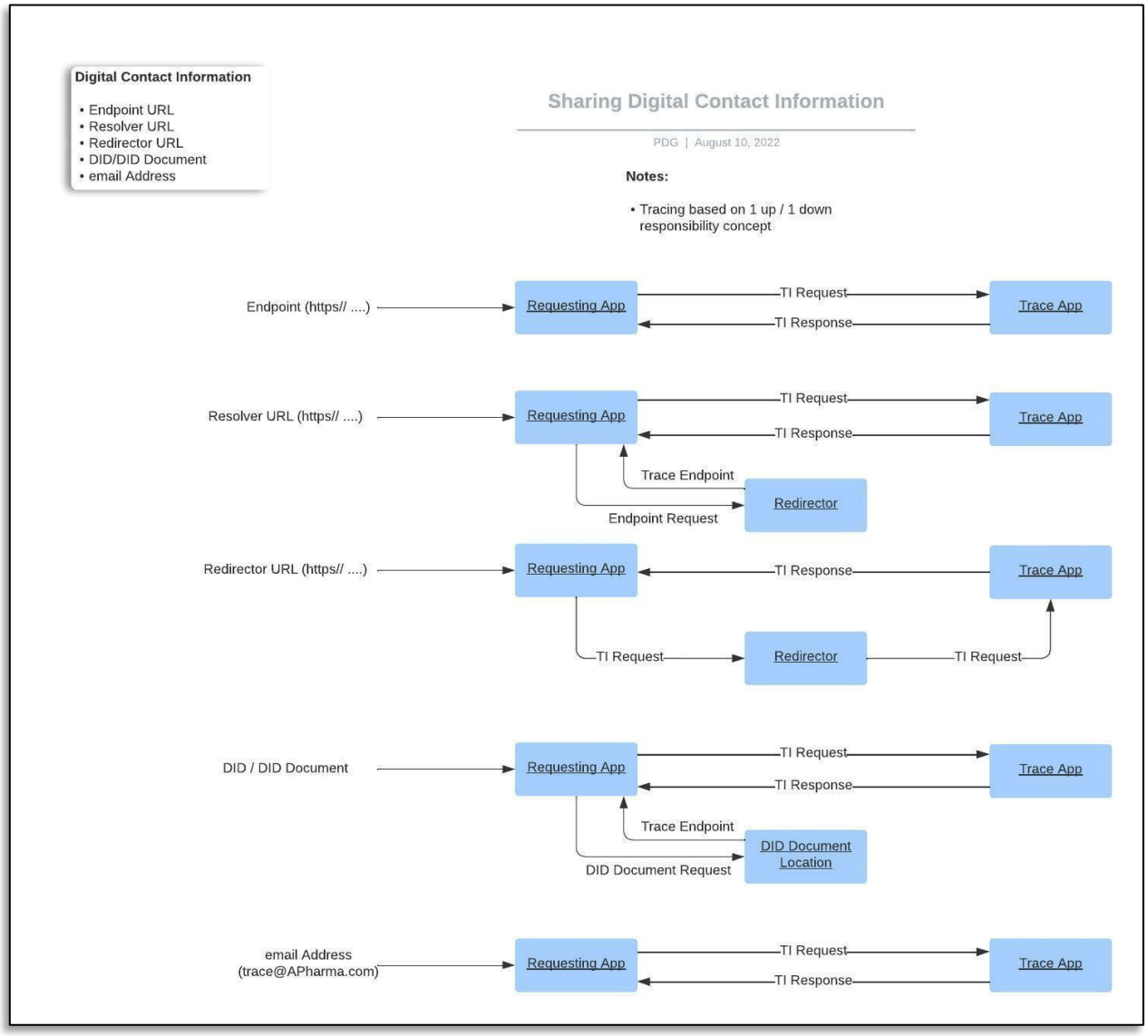

Figure 14 - Trace Endpoint Acquisition Potentiel Options

Recommendations

Although the current PDG-defined tracing architecture is flexible and allows for several methods to exchange TI Request and Response messages (email, OpenAPI, DIDComm, etc.), it is expected that the next phases beyond this functional design (piloting, standardizing, implementation) will provide opportunity for increased interoperability and efficiencies by increasing network-wide standardization and mitigating methods that contribute to data quality issues.

PDG expects this architecture to be refined through Piloting and standardization activities. To support and provide momentum to the development and adoption of interoperable tracing solutions, PDG recommends:

1. Trading Partners and Tracing solution providers pilot the defined TI Request / TI Response messages and choreographies documented in this chapter including:
    a. Assessment of trace volumes,
    b. trial of TI Request/Response messaging and
    c. trial of exchange mechanisms
2. GS1 US uses the PDG Tracing model, schemas and choreographies to develop appropriate standard(s) and guideline(s) similar to the GS1 US Implementation Guide developed for PI Verification.

Exchange interface methods and the use of OCI specified credentials are expected to mature and standardize over the transition/adoption period. Examples of how the JSON schemas and credentials might be piloted, assessed and adopted through mature, industry-wide implementations are listed below. Manual processes, by definition, take place outside of the PDG-defined EDDS [electronic] network.

Configurations Under Consideration

Figure 15 illustrates some implementation variations that are expected to be explored in the next phase (pilot phase) of development in the realization of the PDG-defined EDDS network. Consideration of trading partner and solution provider capabilities may necessitate a transition period for providing initial trace capability and maturing into mature system support.

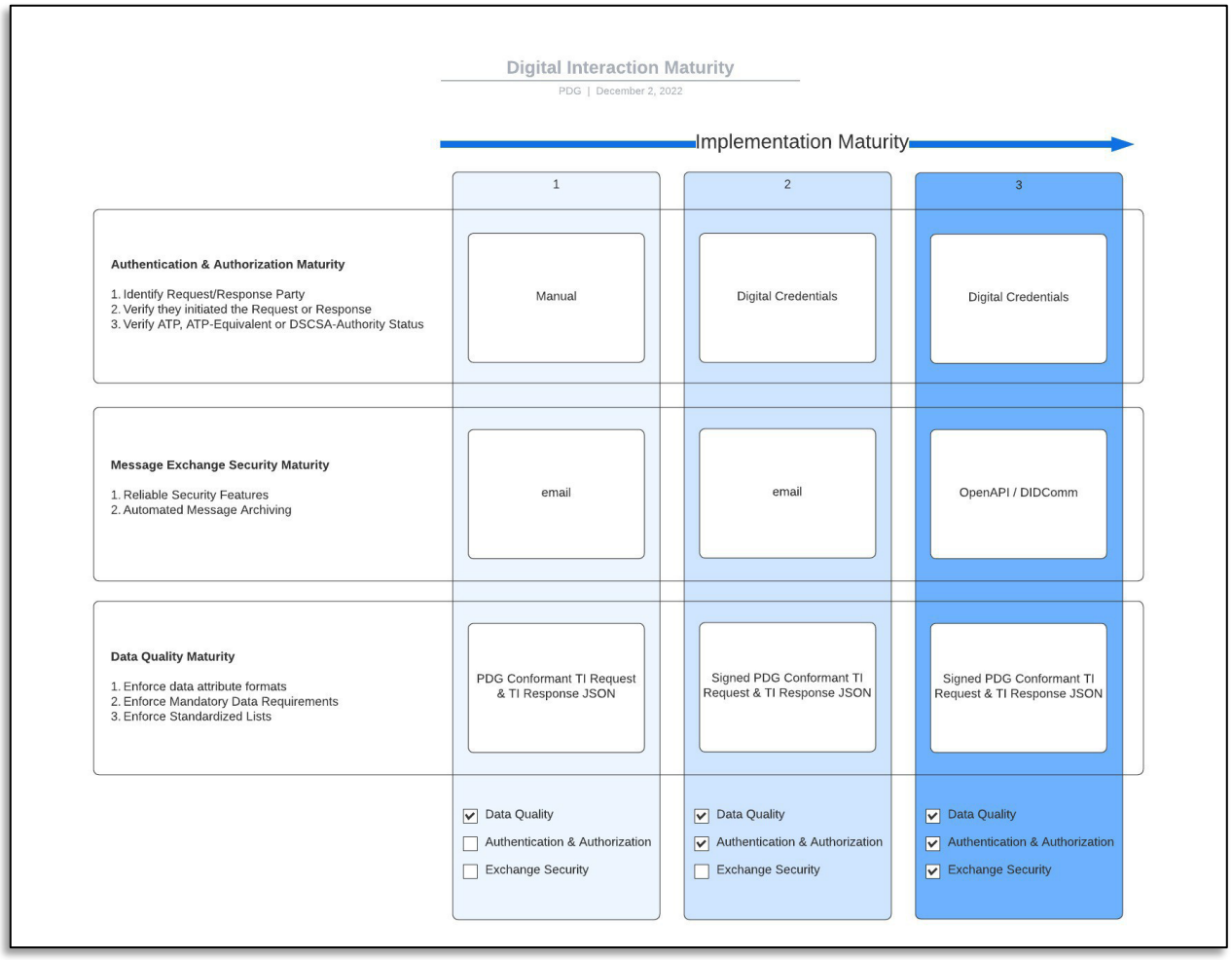

Figure 15 - Trace Network Implementation Maturity

Considerations

Understanding Trace information

Tracing attempts to reconstruct the ownership path of a drug case or package, however, there are instances where available TI data may not tell the full story of each case or package. Requesters and Responders are encouraged to communicate these occurrences outside of the EDDS system using the contact information provided in the TI Request and TI Response messages. The following supply chain scenarios create possibilities of ownership gaps in TI and TS exchanged data:

Returned Product

Each trading partner must provide TI when transferring ownership, however buyers are not required to provide a TI record to the supplier they returned it to. The Buyer's TI data will reflect that the ownership of the case or package was transferred to them, however there will be no TI documenting the transfer back to the supplier. Likewise, the Supplier's TI records might reflect the product being transferred from them twice.

Dispensed, Destroyed or Expired Product

Several situations exist where a product appropriately leaves the supply chain and DSCSA-recorded ownership is ended. There is no additional TI available.

Intracompany Transfers

Trading partners are not required to record and exchange TI records if the product is transferred to another part of the owning or controlling company. The inbound TI and outbound TI may be held in different subsidiary systems.

Figure 16 Illustrates intercompany transfer scenarios based on DSCSA TI and TS exchange strategies of two wholesalers.

Scenario 1: Wholesaler 1 establishes the parent company (HQ) as the Transfer-To party for all their purchases and Transfer-From party for their sales. Wholesaler 1 has two subsidiary companies (1A and 1B).

1. The Manufacturer sells product to Wholesaler 1 (HQ) and ships to its subsidiary, Wholesaler 1A.
2. The Manufacturer's TI and TS reflects the Manufacturer as the Transfer-From entity and Wholesaler 1 (HQ) as the Transfer-To party (they may reflect 1A as the Ship-To party in their EPCIS shipping event).
3. Intracompany transfers occur between Wholesaler 1A and Wholesaler 1B. No TI and TS is exchanged between 1A and 1B.
4. Wholesaler 1 sells product to the Dispenser and ships the product from its 1B subsidiary location.
5. Wholesaler 1's (HQ) TI and TS reflects Wholesaler 1 as the Transfer-From entity and the Dispenser as the Transfer-To party (they may reflect 1B as the Ship-From party in their EPCIS shipping event).

When tracing of products transacted by Wholesaler 1 occurs, Wholesaler 1's system holds TI and TS records that explicitly link the purchased items and sold items with Wholesaler 1, even though intracompany transfers occurred.

Scenario 2: Wholesaler 2 has two subsidiary companies (2A and 2B). Wholesaler 2 establishes the subsidiary company Wholesaler 2A as the Transfer-To party for all their purchases. Product is exchanged between Wholesaler 2A and Wholesaler 2B (sibling subsidiaries). Wholesaler 2B is established as the Transfer-From party for their sales.

1. The Manufacturer sells product to Wholesaler 2A (subsidiary of Wholesaler 2) and ships to Wholesaler 2A.
2. The Manufacturer's TI and TS reflects the Manufacturer as the Transfer-From entity and Wholesaler 2A as the Transfer-To party (they may also reflect 2A as the Ship-To party in their EPCIS shipping event).
3. Intracompany transfers occur between Wholesaler 2A and Wholesaler 2B. No TI and TS is exchanged between 2A and 2B.
4. Wholesaler 2B sells product to the Dispenser and ships the product from its location.
5. Wholesaler 2B's TI and TS reflects Wholesaler 2B as the Transfer-From entity and the Dispenser as the Transfer-To party (they may also reflect 2B as the Ship-From party in their EPCIS shipping event).

When tracing of products transacted by Wholesaler 2's subsidiaries occurs, Wholesaler 2A's system holds TI and TS records that explicitly link the purchased items with Wholesaler 2A. Wholesaler 2B's TI and TS system holds records that explicitly link the sold items with Wholesaler 2B. It is in Wholesaler 2's best interest to establish records of intracompany transfers for DSCSA tracing purposes, otherwise, a TI Request initiated by the Dispenser, to Wholesaler 2B may not return the TI issued by the Manufacturer to Wholesaler 2A, breaking the TI trace collection.

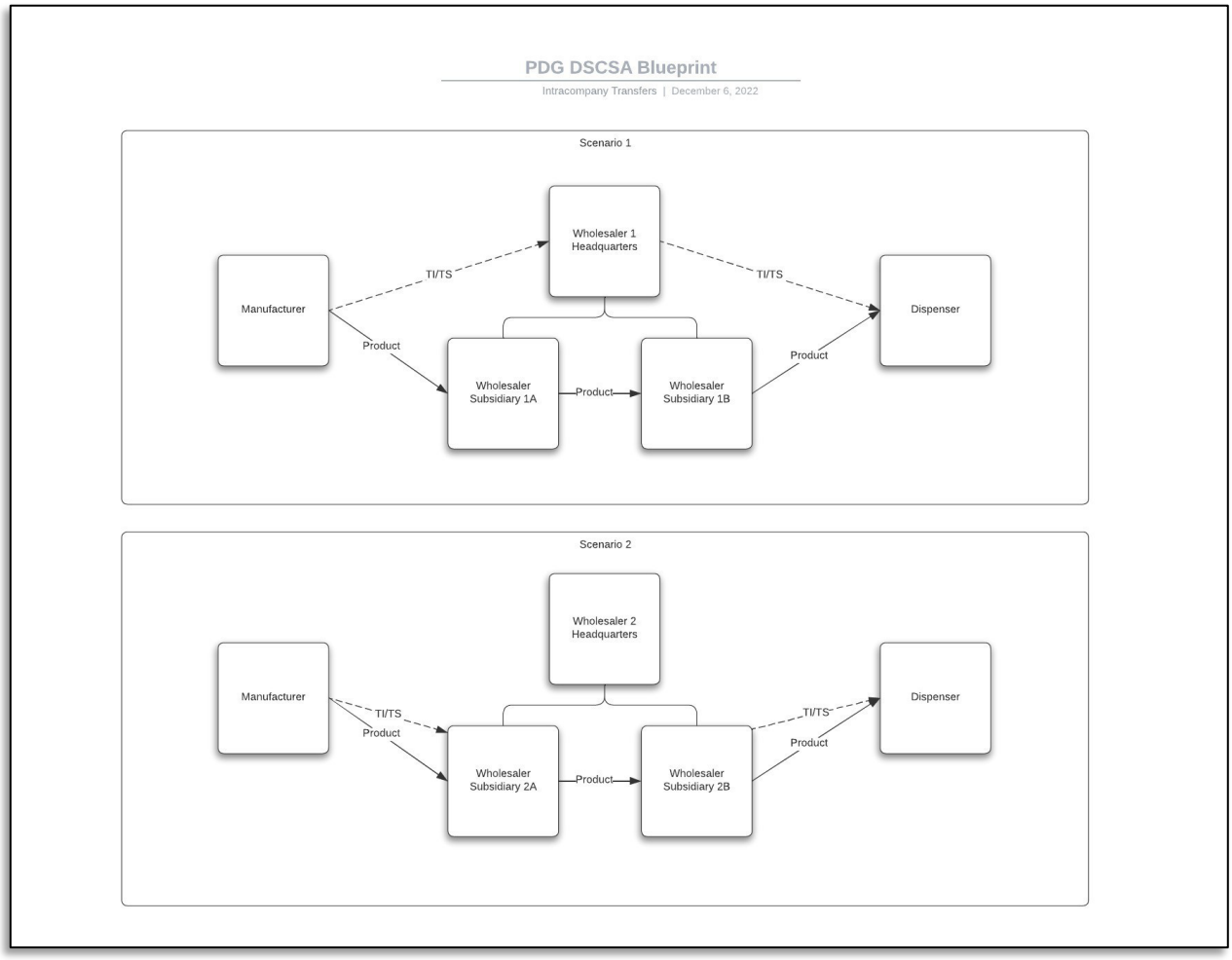

Figure 16 - Illustrations of Intracompany Transfers

Repackaged Product

Sec. 582(e)(2)(A)(iv) of the statute requires Repackagers to *"associate the product identifier the repackager affixes or imprints with the product identifier assigned by the original manufacturer of the product"*. This association information is not TI data (ownership transfer) and will not be reflected in a TI Response to a TI Request for either the original manufacturer's product or the repackaged product.

Misalignment Exceptions and Tracing

Chapter 3 – TI and TS exchange includes guidance on managing misalignment exceptions. The result of misalignment exceptions management may result in replacement TI record(s), however, some exceptions may not and may affect a trading partner's ability to provide trace information.

Implementation Considerations

1. To mitigate against inducing duplicate work for Responders and duplicate archive records for Requesters and Responders, Trace Solutions should consider checking if the Trace has already been submitted.
2. Responders and Requesters can use the Contact Information in the TI Request, TI Response, or any other means to contact and interact with the Requester.
3. The Requester has requested an item and expects TI or ownership information in response. Suppose the Responder doesn't hold any Transaction Information for the item. In that case, the Responder or Requester may follow up using the contact information:
    a. Requester may have made a mistake in entering the request
    b. Requester may follow up separately if they believe the Responder should have TI.
    c. Responder may follow up to ensure a mistake has been made.
    d. Responder may follow up to investigate the request further.
4. A Responder might contact the Requester using the Contact Information if receiving a TI Request for "Illegitimate Product Investigation" purposes is the first time the Responder is aware of the investigation.
5. Systems generating trace requests routed to or alerted by emails should include the ability to monitor for spam and inform users to mark email addresses as safe.
6. Responders may warn of duplicate requests and respond to the [duplicate] request.
7. Tracing Records Retention: TI Request and TI Response messages may be considered part of an investigation. In that case, Requesters and Responders must comply with DSCSA data archiving requirements of data retention for six (6) years after an investigation.
8. If the nature of the Request needs to be communicated, the Requester may use investigation circumstances in the TI Request. A Requester may also TI request additional information that may be used to provide additional documentation.
9. The Responder system will acknowledge receipt of the request.
10. The responder can respond with ReqItem-003, Response Delayed, providing the Requester with the Responder's contact information.
11. **Decision to respond:** The Responder may contact the Requester using the contact information provided in the TI Request.
12. Scanning products to acquire Product Information should minimize errors
13. Requester should check the Responder's contact information for responses they don't expect.
14. Solutions should provide a means of managing old requests/responses via archiving, sorting, etc.
15. Before receiving a response, if a Requester determines that the response is no longer needed, the Requester may contact the Responder to cancel the request. The Responder may respond using RL-001 Request Closed to close the request formally.

ID	Functional Requirement
Trace-FR-001	Trading partners (ATPs and ATP Equivalents) SHALL provide their Trace Endpoint to their customer and supplier trading partners.
Trace-FR-002	Should a company's Trace Endpoint change, trading partners (ATPs and ATP Equivalents) SHALL provide their updated Trace Endpoint to their customer and supplier trading partners.
Trace-FR-003	Trading Partners (or their Solutions) SHALL retain Trace Request and Response records for 6 years after a Suspect Product Investigation or Illegitimate Product investigation.
Trace-FR-004	A TI Request May include requests for one or more Product ID[22] / Serial Number pair.
Trace-FR-005	A TI Request Must indicate a single investigation type (Suspect, Illegitimate or Recall), or compliance audit
Trace-FR-006	Suspect Product Investigations SHALL only allow for package or case level requests.
Trace-FR-007	Illegitimate Product Investigations SHALL only allow for package or case level requests.
Trace-FR-008	Recalled Product Investigations SHALL only be submitted from a DSCSA Authority AND allow for package or case level requests or Lot level requests.
Trace-FR-009	A set of TI Requests SHALL only specify a GTIN/Serial Number pair, a NDC/Serial Number Pair, a GTIN/Lot Number pair (Recalls) or a NDC/Lot Number pair (Recalls).
Trace-FR-009	Responders may need additional time for a particular Product ID / Serial Number request. If that is the case, a response of "Response Pending" is given and a Response is provided later. This does not relieve trading partners of turnaround time as specified in the DSCSA (24 hrs) or FDA Guidances.

[22] GTIN or NDC.

Trace-FR-010	If a response is given for a particular item, and you later need to correct or provide additional data, a replacement or additional response can be made.
Trace-FR-011	Responders Shall return the “No TI Response” message if they do not have TI records for a particular request.
Trace-FR-011	Trace solutions implementing the TI Request and TI Response via OpenAPI, DIDcomm,etc.) shall implement a connectivity check.
Trace-FR-012	If trading partners are using email to transport TI Requests and TI Responses, an acknowledgment of the TI Request or TI Response SHALL be sent to the requester or responder.
Trace-FR-013	TI Request and TI Response message formats shall conform to a standardized message structure based on PDG-defined EDDS network’s JSON schemas for tracing.

Open Issues

ID	Issue
Trace-Issue-001	Architecting a means for DSCSA Authorities to acquire Trace Endpoints
Trace-Issue-002	Establish POT, POC, Pilot(s) to exercise and validate the JSON TI Request and TI Response messages.
Trace-Issue-003	Provide the TI Request and TI Response messages and choreography to GS1 US for standardization process.
Trace-Issue-003	Establish a sunrise date for mandatory use of digital credentials (ATP, ATP-Equivalent and DSCSA Authority) within the PDG-defined EDDS network.
Trace-Issue-004	Addressing how trading partners respond to a request in situations where available TI data does not reflect the true ownership of a case or package.

Appendix A

Term/Acronym	Definition	Notes
TI and TS Trace	The aggregate of a series of TI and TS data gathered from trading partners about a package or case. The Requester may continue gathering individual TI and TS datasets until the needs of their investigation are satisfied. Each subsequent Responder provides information based on the TI and TS data sets they have been sent[23] or have sent to their suppliers and customers.	
TI Requester or Requester	Represents the ATP, ATP-Equivalent or DSCSA Authority requesting TI from an ATP or ATP-Equivalent entity, usually through their TI Request/Response system.	
TI Responder or Responder	Represents the ATP or ATP-Equivalent responding to TI Requests from an ATP, ATP-Equivalent or DSCSA Authority, usually through their TI Request/Responding system.	
DSCSA Trace Solution	A computer application used to create, store and exchange TI requests and TI Responses. TI Request/Response systems must be able to interoperate with other TI Request/Response systems and Digital Wallets. These applications may be built in-house or supplied by a Solution Provider.	
DSCSA Enabled Digital Wallet	An application or service supporting Verifiable Credentials, Decentralized Identifiers and specific interactions supporting PI Verification and Tracing.	
Trace Endpoint	A Trace Endpoint is the electronic address where an ATP or ATP-Equivalent receives electronic TI Requests conformant with the PDG TI Request message[24]. In the TI Response message[25] the Trace Endpoint is either the digitalContactEmailAddress or the digitalContactURIAddress.	

Standards, Specifications, and Guidelines

Currently, there are no standards for tracing that meet the requirements laid out in the DSCSA statute and the Tracing section of Chapter 1 of the PDG Blueprint. PDG has developed a set of draft JSON schemas representing a TI Request and TI Response that are appropriate for proof of concepts and piloting. The

[23] For the purposes of this document, having possession of a TI and TS dataset and having access to a TI and TS data set represent the transfer of TI and TS and carry the same meaning.
[24] *Appendix 1 – TI Request JSON Schema.*
[25] *Appendix 2 – TI Response JSON Schema.*

Recommendations section calls for PDG to request GS1 US to use these schemas as a starting point to develop formal standards and guidelines for use to support DSCSA requirements.

Table 1 – Tracing Reference Documents

Reference Document	Version	Publisher	Notes
PDG TI Request Message (JSON)	PoC v13	PDG	
PDG TI Response Message (JSON)	PoC v14	PDG	

Change Control

Date of Change	Section	Description of Change	Approved By
Version 1.2			
4/4/2023	Ch. 5 Table 1 and Schemas	Corrections and additions of schemas	PDG Board of Directors
Version 1.3			
8/28/2023	Ch. 5	Changed “TI/TS” to “TI and TS	PDG Board of Directors
Version 1.4			
		No changes from the prior version	
Version 1.5			
1/15/2026	Ch. 5	Corrected message codes (replaced temporary codes). Removed Table 1: TI Request and Response Data Attributes and published the content as a separate “Glossary” document. Removed overly complex data hierarchy diagrams. Added usage disclaimer language. Added Implementation Considerations.	PDG General Members
Version 1.6			
		No changes from prior version	