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

Chapter 1: Understanding of Compliance Requirements and Baseline Business Requirements

Version 1.3
January 16, 2024

pdg Partnership for DSCSA Governance

About PDG

The Partnership for DSCSA Governance (PDG) is a collaborative forum and FDA public-private partnership dedicated to developing, advancing, and sustaining an effective and efficient model for interoperable tracing and verification of prescription pharmaceuticals in the U.S., as required by the Drug Supply Chain Security Act (DSCSA). PDG's membership includes leading authorized manufacturers, repackagers, wholesalers, third-party logistics providers, and dispensers (hospitals and retail and independent pharmacies), as well as leading industry trade associations and technical experts. Together, these members are working to establish a comprehensive vision for industry's implementation of the DSCSA and enhance pharmaceutical supply chain security in the interest of patient safety for generations to come. For more information, visit www.DSCSAgovernance.org.

PDG Members

Accenture
Advasur, LLC
American Pharmacists Association (APhA)
Apotex Corp.
Association for Accessible Medicines (AAM)
AstraZeneca
Be4ward Ltd
Blue Link ERP
Bristol Myers Squibb
Cardinal Health
Cleveland Clinic
Cencora
ConsortiEX, Inc.
CVS Health
Eli Lilly and Company
Emergent BioSolutions
Endo Pharmaceuticals
Eversana Life Sciences, LLC
Excellis Health Solutions
E2E VISIBILITY, Inc.
Gateway Checker
Geisinger Health
Genentech
Gilead Sciences, Inc.
Harmony Biosciences Holdings, Inc.
Healthcare Distribution Alliance (HDA)
Hercules Pharmaceuticals, Inc.
InfiniTrack, LLC
Inmar, Inc.
International Warehouse Logistics Association (IWLA)
Johnson & Johnson Services, Inc.
Ledgerdomain, LLC
Legisym, LLC
LSPediA Inc.
McKesson Corporation
Medline Industries
Meijer Pharmacy
Movilitas Consulting, LLC
National Association of Boards of Pharmacy (NABP)
National Community Pharmacists Association (NCPA)
Novo Nordisk, Inc.
OrderInsite
Pfizer, Inc.
Pharmaceutical Research and Manufacturers of America (PhRMA)
Providence Health Technologies, LLC
rfxcel Corporation
Sam's Health Mart
Sanofi
SAP SE
Second Generation LTD
Spherity
Systech
OrderInsite
Paul Consulting
TraceLink Inc.
Two Labs
UNC Health
Uptown Pharmacy
Walgreen Co.
Walmart Inc.
Vine Meds LLC

Table of Contents

Future Chapters Forthcoming

About this Document

Efficient implementation of the Drug Supply Chain Security Act (DSCSA) will benefit from an intentional implementation plan that builds toward a shared blueprint for 2023 interoperability.[1] As the pharmaceutical supply chain industry looks toward 2023, the Partnership for DSCSA Governance (PDG)[2] has collaborated with industry stakeholders to develop a Foundational Blueprint for 2023 Interoperability.[3] Importantly, PDG's Foundational Blueprint for 2023 Interoperability is intended to highlight the complexities and the importance of cross-industry governance[4] and collaboration in meeting the 2023 DSCSA requirements. To this end, the requirements, and recommendations as set forth below, which are contained in PDG's Foundational Blueprint should not be taken as a requirements and recommendations only for members of PDG. As an independent, balanced, and sector-neutral governance body, PDG believes this initial output from months of collaboration will begin to provide the necessary certainty and longevity of an effective implementation plan for the DSCSA 2023 requirements.[5]

This document sets forth the PDG-defined compliance requirements and business requirements for 2023 interoperability.[6] They are captured in the form of requirements and recommendations. *"***Requirements"** shall or must be done to implement the PDG blueprint. "**Recommendations"** encouraged or should be done to implement the PDG blueprint.

Some of the requirements identified in this blueprint are compliance requirements, representing characteristics of proposed systems and processes that are necessary to meet the statutory obligations of the DSCSA. Other requirements in this blueprint are business requirements, representing technical characteristics of proposed systems and processes that are operationally necessary to satisfy a compliance requirement. Individual companies' legal interpretations of the specific scope compliance may differ, PDG believes all of the requirements in this document are practically necessary to efficiently achieve interoperability as intended by the DSCSA.

It is important to note that PDG is not a governmental entity or agency thereof and therefore does not represent the views or positions of the government or enforcement agencies. The work of PDG does not carry the force of law. The DSCSA expressly permits trading partners[7] to adopt "alternate methods of compliance," and the PDG blueprint is not intended to foreclose that option. Trading partners can implement the DSCSA requirements and comply fully with the DSCSA without implementing the PDG blueprint. PDG's goal simply is that its blueprint can serve as an optimal approach to implementation that trading partners will opt to follow.

[1] The term "interoperability" is further defined in the glossary.
[2] The term "PDG" is further defined in the glossary.
[3] The term "Foundational Blueprint for 2023 Interoperability" is further defined in the glossary.
[4] Governance includes the successful collaboration of all supply chain sectors in the establishment of efficient, viable, and effective systems and processes to protect patients through compliance with the DSCSA 2023 requirements. As discussed below, adoption of the principles described in this document is voluntary.
[5] The term "DSCSA 2023 requirements" is further defined in the glossary.
[6] The term "business requirements and recommendations" is further defined in the glossary.
[7] The term "trading partner(s)" is further defined in the glossary.

Chapter 1: Understanding of Compliance Requirements and Baseline Business Requirements

Drug traceability is a highly technical and detailed topic and the systems and processes necessary to implement it are complex. The DSCSA, for the most part, provides only general requirements and leaves many of the details of implementation to industry and/or FDA. Recognizing the divergence between statute and practice, this Chapter provides PDG's general understanding of the statutory requirements of the DSCSA and defines baseline business requirements that frame the general systems and processes for implementation of the main components of the DSCSA: (1) secure, electronic, interoperable systems and processes for the exchange of serialized transaction information (TI) and transaction statements (TS), (2) secure, electronic, interoperable systems and processes for product-identifier verification, and (3) secure, electronic, interoperable systems and processes for tracing.

Requirements and Recommendations to Support Serialized TI and TS Data Exchange

Under the DSCSA, trading partners must provide transaction information to the subsequent owner of a product "prior to, or at the time of, each transaction."[8] In addition, beginning November 27, 2023, all TI and TS must "be exchanged in a secure, interoperable, electronic manner in accordance with the standards[9] established [through FDA guidance]," and the TI must "include the product identifier[10] at the package level for each package included in the transaction."[11] In addition to being a direct statutory requirement, the electronic, interoperable exchange[12] of TI is also foundational to achieving electronic interoperable tracing[13] and verification[14], as required by the DSCSA.

TI and TS are being electronically exchanged today at the lot-level, typically via an advance ship notice (ASN). The addition of the product identifier to TI in 2023, however, will require the inclusion of serial number and expiration date in the TI. The ASN, *as currently structured*, does not accommodate those elements. Trading partners, therefore, must identify and implement new systems[15] and process for exchange of TI that accommodates the serial number and expiration date. Within the commercial business environment, there has been significant movement toward GS1 Electronic Product Code Information Services (EPCIS) standards[16] as a preferred method of exchange between manufacturers and wholesale distributors. In fact, most manufacturers and wholesale distributors have already begun implementation of EPCIS. Among dispensers, there has been a greater diversity of plans.

The need for an updated method of TI exchange—whether that method is EPCIS or some alternative—presents the opportunity to enhance the standardization of the TI content and enable greater interoperability. Accordingly, this initial Chapter focuses on this "what" component of the TI content: what standardized format will TI follow to enable interoperability. We anticipate that future PDG work will focus on the "how" component of TI exchange methods that enable two trading partners to exchange TI in those formats.

[8] The term "transaction" is further defined in the glossary.
[9] The term "standard(s)" is further defined in the glossary.
[10] The term "product identifier" is further defined in the glossary.
[11] Food Drug & Cosmetic Act (FDCA) § 582(g)(1)(B).
[12] The term "interoperable exchange" is further defined in the glossary.
[13] The term "interoperable tracing" is further defined in the glossary.
[14] The term "verification" is further defined in the glossary.
[15] The term "system(s)" is further defined in the glossary.
[16] The term "ECPIS" is further defined in the glossary.

Standards and Methods of Exchange	
Requirement/Recommendation ID	**Requirements/Recommendation**
Requirement-Ser-001	Authorized Trading Partners (ATPs), when exchanging TI for an individual transaction of a product, shall exchange the 13 data elements (specified below in Requirements-Ser-003 to -024) comprising TI in machine-readable (as defined in the glossary) data.
Requirement-Ser-002	ATPs shall ensure the TI and TS data elements they provide, capture, and maintain can be exposed/communicated in a consistent format (specified in Reqs-Ser-003 to 024) as part of the process for interoperable verification[17] and/or interoperable tracing.
TI Element Formats	
(1) Proprietary or Established Name or Names	
See notes below on contextual elements of TI	
(2) Strength	
Requirement-Ser-003	Strength shall be expressed as the amount of active pharmaceutical ingredient (API) and corresponding unit of measure.[18]
(3) Dosage Form	
Requirement-Ser-004	Dosage form shall be expressed as the product[19] in its physical form.
(4) Container Size	
Requirement-Ser-005	Container size shall be expressed as quantity and unit of the individual saleable unit.
(5) Number of Containers	
Requirement-Ser-006	Number of containers is the number individual saleable units and shall be expressed as a numeric value.[20]
Requirement-Ser-007	When exchanging the number of containers of the product in machine readable data, the machine-readable value shall be formatted as a numeric value (base-10).
Recommendation-Ser-008	When presenting the number of containers of the product in human readable form, the human readable value should be formatted as a numeric value (base-10).
(6) National Drug Code (NDC)	
Requirement-Ser-009	When exchanging the NDC number of the product in machine readable data, the machine-readable value shall be formatted as the FDA-assigned 10-digit[21] NDC, including hyphens.

[17] The term "interoperable verification" is further defined in the glossary.
[18] For example, if a 5ml 1g vial is transacted, the strength is 200mg/ml.
[19] Note this is the "product" not the "package."
[20] The number of containers may vary depending on what is represented by the TI. If the TI represents the exchange of ownership of multiple saleable units, this will be the calculated quantity of individual saleable units of the GTIN. If the TI represents an individual sGTIN (e.g., when tracing a specific sGTIN), the number of containers will always be "1."
[21] The FDA notes in its March 2018 draft guidance that the number of containers should be the quantity of individual saleable units of a product of the same lot number that is included in a transaction. To the extent that more than one lot number is associated with the products received in a transaction, the products should be grouped by lot number, and the number of containers for each group of lot numbers should be reflected on the transaction information provided to the subsequent purchaser.

Requirement-Ser-010	When presenting the NDC in human readable form, the human readable value shall be formatted as the FDA-assigned 10-digit[22] NDC, including hyphens.
(7) Lot Number	
Requirement-Ser-011	When exchanging the lot number in machine readable data, the machine-readable value shall be formatted as a variable alphanumeric (including special characters and case-sensitive) value up to 20-characters consistent with the lot number expressed on the human-readable packaging. The lot number format shall be in accordance with the allowable characters specified in the GS1 General Specifications for the application identifier for lot number. The machine-readable value shall exclude prefixes and/or suffixes that are not on the human-readable packaging.
Requirement-Ser-012	When presenting the lot number in human-readable form, the human-readable value shall be formatted as a variable alphanumeric (including special characters and case-sensitive) value up to 20-digits consistent with the machine-readable value. The lot number format shall be in accordance with the allowable characters specified in the GS1 General Specifications for the application identifier for lot number. The human-readable TI value shall exclude prefixes and/or suffixes that are not on the human-readable packaging.
(8) Date of Transaction	
Requirement-Ser-013	When exchanging the date of the transaction in machine readable data, the machine-readable value shall be formatted according to xsd: dateTime / UTC Time Zone.
Requirement-Ser-014	When presenting the date of the transaction in human-readable form, the human-readable value shall include a year, month, and non-zero day in YYYY-MM-DD format if using only numerical characters or in YYYY-MMM-DD if using alphabetical characters to represent the month. The date shall use a hyphen or a space to separate the portions of the date.
(9) Date of shipment if more than 24 hours after date of transaction	
Requirement-Ser-015	When exchanging the date of shipment in machine readable data, the machine-readable value shall be formatted according to xsd: dateTime / UTC Time Zone.
Requirement-Ser-016	When presenting the date of shipment in human-readable form, the human-readable value shall include a year, month, and non-zero day in YYYY-MM-DD format if using only numerical characters or in YYYY-MMM-DD if using alphabetical characters to represent the month. The date shall use a hyphen or a space to separate the portions of the date.

[22] FDA-assigned NDCs are currently 10 digits in length, but FDA anticipates the length of the NDC to be extended in the near future.

(10) Business name and address of the person from whom ownership is being transferred	
Recommendation-Ser-017	When exchanging the business name and address of the person from whom ownership is being transferred[23] in machine readable data, it is recommended that the name and address be conveyed in 8 fields: 1. name (i.e., business name) 2. streetAddressOne 3. streetAddressTwo (can be blank) 4. streetAddressThree (can be blank) 5. city 6. state 7. postalCode 8. countryCode. It is recommended that the format of the 8 name and address fields follow the USPS Postal Addressing Standards[24] and ISO 3166 for the countryCode.
Recommendation-Ser-018	When presenting the business name and address of the person from whom ownership is being transferred in human-readable format, it is recommended that the name and address be formatted using the USPS Postal Addressing Standards broken into multiple fields.
(11) Business name and address of the person to whom ownership is being transferred	
Recommendation-Ser-019	When exchanging the business name and address of the person to whom ownership is being transferred in machine readable data, it is recommended that the name and address be conveyed in 8 fields: 1. name (i.e., business name) 2. streetAddressOne 3. streetAddressTwo (can be blank) 4. streetAddressThree (can be blank) 5. city 6. state 7. postalCode 8. countryCode. It is recommended that the format of the 8 name and address fields follow the USPS Postal Addressing Standards[25] and ISO 3166 for the countryCode.
Recommendation-Ser-020	When presenting the business name and address of the person to whom ownership is being transferred in human-readable format, it is recommended that the name and address be formatted using the USPS Postal Addressing Standards broken into multiple fields.

[23] As explained further in the accompanying *Background, Context, and Reflection* document, Recommendations-Ser-017 and -018 provide recommended address *format* regardless of the specific type of address, whether a corporate address or a shipping location.
[24] The USPS Postal Addressing Standards are available at https://pe.usps.com/cpim/ftp/pubs/pub28/pub28.pdf.
[25] *Id.*

(12) Standardized Numerical Identifier (SNI)	
Requirement-Ser-021	When exchanging the Standardized Numerical Identifier in machine readable data, the machine-readable value shall be exchanged as the serialized Global Trade Item Number (sGTIN) formatted according to the GS1 General Spec and GS1 US Implementation Guideline for Applying GS1 Standards for DSCSA R1.2.
Requirement-Ser-022	When presenting the Standardized Numerical Identifier in human-readable form, the human-readable value shall be formatted as the sGTIN with the serial number and GTIN displayed as two fields: (i) the GTIN-14 with no dashes, and (ii) the serial number.
(13) Expiration Date	
Requirement-Ser-023	When exchanging the expiration date of the product in machine readable data, the machine-readable value includes a year, month, and non-zero day[26] and shall be formatted using the XML standard (YYYY-MM-DD).[27]
Requirement-Ser-024	When presenting the expiration date of the product in human-readable form, the human-readable value shall include a year, month, and non-zero day in YYYY-MM-DD format if using only numerical characters or in YYYY-MMM-DD if using alphabetical characters to represent the month. The date shall use a hyphen or a space to separate the portions of the date.
Virtual/Physical Alignment	
Requirement-Ser-025	Each trading partner shall have controls (*i.e.*, systems and processes) in place to ensure its physical supply chain (as defined in the glossary) is reliably consistent with its virtual supply chain (as defined in the glossary), but individual trading partners may choose, as a matter of business practice, the exact controls it will use, including how and where those controls are implemented in the trading partner's processes.
Requirement-Ser-026	Each trading partner shall have systems and processes in place to identify[28], understand[29], and resolve[30] misalignment exceptions[31] (*e.g.*, the physical supply chain includes one or more packages where the product identifiers are not accurately reflected in the TI, the virtual supply chain includes one or more product identifiers that do not

[26] It is not uncommon for FDA to extend the expiration date for certain products in the event of a drug shortage. In those instances, the "functional" expiration date differs from the expiration date in the product identifier affixed to the package. The Expiration Date presented in the TI is the expiration date in the product identifier affixed to the product.
[27] Systems can be designed to ensure a non-zero day is used.
[28] Identify means a trading partner identifies that a misalignment exception exists.
[29] Understand means the trading partner that identifies the misalignment exception, in coordination with its trading partners, will take various steps to understand the cause of the misalignment exception, specifically whether the misalignment exception is the result of a data error or reflects the presence of a suspect/illegitimate product.
[30] Resolve means the trading partner that identifies the misalignment exception takes steps to address the exception.
[31] The term "misalignment exceptions" is further defined in the glossary.

	accurately reflect the SNIs affixed to the physical product the TI accompanies).
Requirement-Ser-027	Manufacturers, wholesale distributors, and repackagers shall have systems and processes to limit and detect misalignment exceptions related to physical product sold. The specific systems and processes implemented by each trading partner is an individual business decision.
Requirement-Ser-028	Wholesale distributors and repackagers shall reconcile each physical unit received (saleable unit, or a higher logistics unit, such as a case, if the unit to be sold by the wholesale distributor or repackager is higher than the saleable unit) against the TI that was captured and maintained when the wholesale distributor or repackager accepted ownership of the product. It is an individual business decision when and how the wholesale distributor or repackager performs that reconciliation within its business process.
Requirement-Ser-029	Dispensers shall have systems and processes to either (i) identify misalignment exceptions through inspecting/auditing of physical saleable units received against the TI that was captured and maintained when the dispenser accepted ownership of the product, or (ii) reconcile every physical saleable unit received against the TI that was captured and maintained when the dispenser accepted ownership of the product. It is an individual business decision as to how and when a dispenser conducts a reconciliation of product identifiers.
Requirement-Ser-030	When a misalignment exception is identified, the package(s) at issue shall not be further transacted until the misalignment exception has been understood and resolved.
Requirement-Ser-031	Each individual trading partner shall independently determine the exact systems and processes/methods it will employ to meet Requirements-Ser-025 to -030.
Recommendation-Ser-032	The systems and processes implemented to meet Requirements-Ser-025 to -030 should take into account: 1. The historical performance of the supplier, including a pattern of errors. 2. Whether an organization is outside of the PDG Ecosystem[32] (i.e., a trading partner that ascribes to an alternative approach to interoperability). 3. Whether there is a specific patient risk for the product.

Contextual TI Elements

Certain elements of the TI—specifically, the product name, strength, dosage form, and container size—provide contextual information that is based on and tied to the NDC or GTIN. Because these elements simply provide additional context to the NDC or GTIN, their standardization is not critical to interoperability,

[32] The term "PDG Ecosystem" is further defined in the glossary.

and the significant cost of standardizing those elements across the industry would be difficult to justify. That said, it is also recognized that increased standardization is always desirable where easily achieved. Therefore, as new systems and processes are developed in future years, and new ATPs enter the market and develop new systems and processes, it is useful to identify target formats that can be used to support a long-term pathway to increased standardization. The formats below should not be viewed as affirmative recommendations, but rather as directional points of reference as trading partners evolve their systems and processes over time in ordinary course of business.

Proprietary or Established Name or Names: Machine Readable	When exchanging and/or maintaining the proprietary or established name or names of the product in machine readable data, it is encouraged that the machine-readable[33] value be formatted according to RxNorm (RxCUI) standards.[34]
Proprietary or Established Name or Names: Human Readable	When presenting the proprietary or established name or names of the product in human readable form[35], it is encouraged that the human readable value be formatted according to RxNorm- Semantic Branded Drug and RxNorm- Semantic Clinical Drug standards.
Strength: Machine Readable	When exchanging and/or maintaining the strength of the product in machine readable data, it is encouraged that the machine-readable value be formatted according to Structured Product Labeling for units of measure.[36]
Strength: Human Readable	When presenting the strength of the product in human readable form, it is encouraged that the human readable value be formatted according to Structured Product Labeling for units of measure.
Dosage Form: Machine Readable	When exchanging the dosage form of the product in machine readable data, it is encouraged that the machine-readable value be formatted according to Structured Product Labeling for dosage form.[37]
Dosage Form: Human Readable	When presenting the dosage form of the product in human readable form, it is encouraged that the human readable value be formatted according to Structured Product Labeling for dosage form.[38]
Container Size: Machine Readable	When exchanging the container size of the product in machine readable data, it is encouraged that the machine-readable value be formatted according to Structured Product Labeling for package type.[39]
Container Size: Human Readable	When presenting the container size of the product in human readable data, it is encouraged that the human readable value be formatted according to Structured Product Labeling for package type.

[33] The Open Knowledge Foundation's *Open Data Handbook* defines machine-readable data as "Data as a data format that can be automatically read and processed by a computer, such as CSV, JSON, XML, etc. Machine-readable data must be structured data."
[34] The RxNorm standard is accessible here: https://www.nlm.nih.gov/research/umls/rxnorm/index.html.
[35] Here, human readable means a human readable presentation of TI, not human readable package labeling. "Human readable presentation" means the presentation of the machine readable data in a user interface or as part of a written report, such as, for example, the provision of TI to FDA in response to a request for information.
[36] Accessible here: https://www.fda.gov/industry/structured-product-labeling-resources/units-measure.
[37] Accessible here: https://www.fda.gov/industry/structured-product-labeling-resources/dosage-forms.
[38] The FDA's NDC Directory is available at https://www.accessdata.fda.gov/scripts/cder/ndc/index.cfm.
[39] Accessible here: https://www.fda.gov/industry/structured-product-labeling-resources/package-type.

Requirements and Recommendations to Support Interoperable Verification

The DSCSA requires the implementation of secure, electronic, interoperable systems and processes to verify the product identifier affixed to a product. The DSCSA defines verification as the process of "determining whether the product identifier affixed to, or imprinted upon, a package or homogeneous case[40] corresponds to the standardized numerical identifier . . . assigned to the product by the manufacturer or the repackager."[41]

Manufacturers and repackagers are already required, as of November 27, 2017, to respond to any verification request initiated by any authorized[42] trading partner in possession or control of the product to be verified.[60] The DSCSA 2023 requirements build on that foundation by requiring *secure, electronic, interoperable systems and processes* to carry out that verification. In addition to manufacturers' and repackagers' obligation to respond to verification requests, trading partners are also obligated to perform (*i.e.*, initiate) verification of a product identifier in certain circumstances. Specifically, (i) all trading partners must perform verification of a product identifier as part of their obligation to investigate suspect and illegitimate products[43], and (ii) manufacturers, repackagers, and wholesale distributors must verify saleable returns prior to further transacting the product.

Verification Methods

At its core, verification is the process by which the product identifier affixed to a physical product is confirmed against a data source that reflects valid product identifier data elements that could be affixed to the corresponding product. A critical question, therefore, is which data sources are valid sources against which a product identifier may be verified. Conceptually, there are three data sources against which a product could conceivably be verified.

1. **Direct-to-Source Verification**. A product identifier could be verified against commissioning-level data generated and maintained by the manufacturer or repackager of the product. *PDG recognizes that direct-to-source verification is an appropriate method of verification.*
2. **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. *PDG also recognizes that direct-to-replicate verification is an appropriate method of verification in certain circumstances.*
3. **Direct-to-Product Verification**. A product identifier could (in theory) be verified against a set of data generated by capturing and storing the product identifier information from the product package (e.g., a trading partner could scan product upon receipt to generate a data set that could be used as the source for verification later in the process). *PDG does not believe Direct-to-Product is an appropriate method verification, as "verification" is defined under the statute.*

In recent years, numerous supply chain stakeholders convened by the Healthcare Distribution Alliance (HDA) have developed extensive documentation[44] to support the establishment of the Verification Router Service (VRS). The VRS is an existing method of direct-to-source verification that is currently in use and will continue to be utilized by many trading partners in 2023 and beyond. PDG is assessing whether additional or alternative methods of performing direct-to-source verification are also needed to meet additional use cases, and future chapters of this document will address this issue. Requirements-Ver-002 to -009 are intended to be complementary additions to the existing VRS documentation and work (and would apply equally to other methods of direct-to-source verification if it is determined such alternate methods are needed or appropriate).

[40] The term "homogenous case" is further defined in the glossary.
[41] FDCA § 581(28)
[42] The term "authorized" is further defined in the glossary.
[43] The term "illegitimate product" is further defined in the glossary.
[44] VRS documentation is available at https://www.hda.org/issues/pharmaceutical-traceability.

Requirement-Ver-001	Direct-to-replicate verification shall be an appropriate method of verification only when *all* of the following conditions are met: 1. The trading partner performing the verification purchased the package directly from the manufacturer/repackager (including an exclusive distributor of the manufacturer). 2. The trading partner performing the verification uses commissioning-level data provided directly by the manufacturer/repackager to conduct the verification. 3. The trading partner performing the verification does so only for product in that trading partner's ownership and possession.[45] 4. Direct-to-replicate verification shall not be used for investigation of a product determined to be suspect or illegitimate,[46] as required under DSCSA, or for exceptions processing. 5. The trading partner performing the verification and the manufacturer/repackager utilize processes by which the manufacturer/repackager and the trading partner performing verification will exchange the known statuses identified in Requirements-Ver-003, -004, and -005. If the manufacturer/repackager chooses (optionally) to provide the statuses identified in Requirements-Ver-006, the trading partner shall also account for those statuses as part of the verification.[47]
Requirement-Ver-002	A verification response shall reflect whether the product is unfit for distribution based on the known current status of the product identifier being verified.[48] A status is "known" if it was observed by, or communicated to,[49] the trading partner that is responding to the verification request.[50]
Requirement-Ver-003	A change in product identifier status/condition to "expired" shall be considered "known" to a trading partner and shall be reflected in a related verification response, as required by Req-Ver-002.
Requirement-Ver-004	A change in product identifier status to "recalled" status shall be considered "known" to the manufacturer or repackager of the product and shall be reflected in a verification response by such

[45] Importantly, wholesalers cannot perform verification in response to a verification request from a dispenser against direct-to-replicate data.
[46] For this purpose, a suspect or illegitimate product investigation includes any product deemed suspect or illegitimate by an ATP and any verification performed at the request of a regulator or law enforcement.
[47] Stated differently, the trading partner utilizing direct-to-replicate verification and the manufacturer/repackager have established means to ensure their respective data sets are consistent and aligned with regard to those three specific statuses/conditions. Additional stakeholder discussion is needed in regard to *how* this could be accomplished, recognizing there are existing systems and processes in place today (e.g., the 3911 process and the inclusion of expiration date in the product identifier and TI) to communicate these changes. .
[48] A positive verification does not mean that a product is affirmatively fit for distribution (i.e., saleable); such determination must account for numerous factors in addition to the verification. Instead, a positive verification connotes the *absence* of information that would indicate the product is *unfit* for distribution.
[49] The observation or communication must be at a serial number-level. For example, simply observing that a particular quantity of a given NDC was damaged and non-saleable is not considered knowledge. The event must be observed or communicated in a manner that allows the trading partner to identify the specific sGTIN(s) effected by the event such that the event can be reasonably integrated into the trading partner's DSCSA data repository.
[50] Requirements-Ver-001 to -006 are not intended to describe the way in which a change in status is communicated among trading partners. Rather, these requirements only establish that way in which such changes in status—if and when they have been communicated or observed—are factored into a verification response.

	manufacturer or repackager, as required by Req-Ver-002.
Requirement-Ver-005	A change in product identifier status to "subject to a Form 3911 (other than a 3911 cleared as legitimate product)"[51] status, including a "stolen" status, shall be considered "known" to the manufacturer or repackager of the product and any other trading partner that receives the related Form 3911 and shall be reflected in a related verification response, as required by Req-Ver-002.
Recommendation-Ver-006	It is recommended that trading partners establish systems and processes to communicate changes in product identifier statuses to reflect that the product has been (i) damaged such that it is non-saleable, (ii) destroyed, or (iii) consumed in repackaging activities.
Requirement-Ver-007	Each verification request must include a message type. There are four message types that can be included: (1) saleable return;[52] (2) suspect product[53] or illegitimate product investigation, as required by DSCSA;[54] (3) exceptions processing; and (4) status check.
Requirement-Ver-008	The authorized trading partner initiating a verification request must attest to possession or control of the product being verified. Such attestation must accompany each verification request.
Recommendation-Ver-009	Trading partners should have processes in place to "self-monitor" nefarious verification activity relevant to their business (e.g., ways of determining that the same phishing request was sent to a given manufacturer repeatedly), but the processes deployed should be a business decision.

Requirements and Recommendations to Support Interoperable Tracing

Drug traceability is a core purpose of the DSCSA. Beginning in 2015, and extending until November 27, 2023, trading partners have been required to be able to trace product at the lot level. Primarily, lot-level traceability is achieved through exchange and maintenance of the transaction history (TH). However, in 2023, the TH is statutorily eliminated as a set of data that must be exchanged with each transaction, and instead trading partners must have systems and processes to trace product at the *individual saleable unit* level. Specifically, all trading partners must implement secure electronic interoperable "systems and processes necessary to promptly facilitate gathering the information necessary to produce the transaction information[55] for each transaction going back to the manufacturer" if requested by the FDA, another appropriate official, or an ATP on account of a suspect product or an illegitimate product investigation or a recall.

We define the systems and process for tracing for each of the three statutory use cases, plus the non-regulatory use case of testing necessary to ensure the capability to meet the statutory use cases:

1. Tracing for purposes of investigating a suspect product (Tracing-Suspect)
2. Tracing for purposes of investigating an illegitimate product (Tracing-Illegitimate)
3. Tracing on account of a recall (Tracing-Recall)

[51] The statuses reflected here are conceptual status and do not represent specific standards based language, such as the GS1 Core Business Vocabulary.
[52] Verification of saleable returns is statutorily required.
[53] The terms "suspect product" and "illegitimate product" are further defined in the glossary and the DSCSA.
[54] Verification is statutorily required as part of the suspect product investigation process.
[55] The term "transaction information" is further defined in the glossary.

4. Tracing for compliance audit/testing

For each use case, we recognize three types of actors. An "Initiating Entity" is the ATP or appropriate Federal or State official that initiates the tracing process.[56] "Responding ATPs" are those ATPs that provide data or information in response to a tracing request. The Responding ATPs are generally each of the ATPs that own or have owned the product being traced. "Regulators" are FDA and other appropriate Federal or State officials.

Baseline Requirements for Tracing Systems and Processes	
Direction of Tracing	
Requirement-Trac-001	Systems and processes for Tracing must enable the Initiating Entity to trace the product forward (i.e., transactions subsequent to the first Responding ATP), trace the product backward (i.e., transactions prior to the first Responding ATP), or identify the last ATP known to have owned the product.[57]
Who May Initiate Tracing for What Purpose	
Requirement-Trac-002	Systems and processes for Tracing-Suspect and Tracing-Illegitimate[58] must enable only (i) an ATP involved in the investigation of the suspect or illegitimate product at issue or (ii) a Regulator to act as an Initiating Entity.[59]
Requirement-Trac-003	Systems and processes for Tracing-Recall must enable only a Regulator to act as an Initiating Entity.[60]
Requirement-Trac-004	Any use of systems and processes for tracing for use cases other than those in Requirements-Trac-002 and -003 is a matter of commercial business practice that shall be left to, and would require agreement by, the relevant ATPs.[61]
Level/Granularity of Tracing	
Requirement-Trac-005	Systems and processes for Tracing-Suspect and Tracing-Illegitimate must enable tracing of product by individual sGTIN.
Requirement-Trac-006	Systems and processes for Tracing-Recall may enable tracing of product by individual sGTIN or by IGTIN (lot number and GTIN).[62]

[56] The Initiating Entity is the entity that exercises its legal authority to request that the tracing process be performed.
[57] It is important to read the requirements in this section together as a whole, for example, Requirement-Trac--001 should be read with the understanding that Requirement-Trac--002, -003 and -004 apply and these are all intended to be interdependent. Similarly, Requirement-Trac-001 must be read in conjunction with Requirements-Trac-013 and -014 which make clear no individual ATP is responsible for producing the full information contemplated under Requirement-Trac-001.
[58] It is important to note that these use cases may only by utilized when the product has been declared suspect or illegitimate, which triggers obligations under the DSCSA, such as investigation and quarantine requirements.
[59] It is anticipated that the discussion and development of technical specifications will evaluate the role of credentialing to support this requirement.
[60] It is anticipated that the discussion and development of technical specifications will evaluate the role of credentialing to support this requirement. For clarity, most recalls are expected to be initiated by the manufacturer or repackager as a voluntary recall, and the manufacturer or repackager may be key to starting the tracing *process*; this requirement simply recognizes that the DSCSA give FDA (and other regulators) the authority to request tracing once a recall has occurred.
[61] As a matter of commercial business practice, this activity is outside the scope of PDG's activities.
[62] In developing technical specifications PDG will specifically consider whether there are technical advantages to simultaneously tracing all sGTINs in a lot versus a single tracing process for the lot.

Requirements to Initiate Tracing	
Requirement-Trac-007	To initiate the Tracing-Suspect process, the Initiating Entity shall provide the following: 1. The four elements of the product identifier (GTIN, serial number, expiration date, and lot number).[63] 2. The reason "Suspect Product Investigation." 3. An attestation by the Initiating Entity that the process is being initiated to support a suspect product investigation. 4. If the tracing is being initiated by a Regulator, an attestation that the tracing is being initiated at the request of a Regulator. 5. As optional information, a description of the suspect product investigation.[64]
Requirement-Trac-008	To initiate the Tracing-Illegitimate process, the Initiating Entity shall provide the following: 1. The four elements of the product identifier (GTIN, serial number, expiration date, and lot number). 2. The reason "Illegitimate Product Investigation." 3. The incident number associated with the Form 3911 filed for the illegitimate product. 4. An attestation by the Initiating Entity that the process is being initiated to support an illegitimate product investigation. 5. If the tracing is being initiated by a Regulator, an attestation that the tracing is being initiated at the request of a Regulator. 6. As optional information, a description of the illegitimate product investigation.[65]
Requirement-Trac-009	To initiate the Tracing-Recall process, the Initiating Entity shall provide the following: 1. The GTIN, expiration date, lot number, and if applicable, the serial number(s). 2. The reason "Recall." 3. An attestation by the Initiating Entity that the process is being initiated on account of a recall. 4. A statement that the tracing is being initiated by a Regulator. 5. As optional information, a description of the recall.[66]
Requirement-Trac-010	If a Regulator is the Initiating Entity, the Regulator's request must clearly indicate whether it is a request for TI and TS under § 582(g)(1)(D) or a request under § 582(g)(1)(E)(i) to promptly facilitate gathering the information necessary to produce the TI for each

[63] Pursuant to widely recognized international standards, the GTIN is encoded in the product identifier. Recognizing the FDA's reliance on NDC, continued discussion of technical specifications will address the interchangeability of, or methods for crosswalk to, the NDC.
[64] Subject to confirmation that this will not impede interoperability or automation. Additionally, it is anticipated that the discussion and development of technical specifications will consider how a point-of-contact or other information can be incorporated.
[65] Subject to confirmation that this will not impede interoperability or automation. Additionally, it is anticipated that the discussion and development of technical specifications will consider how a point-of-contact or other information can be incorporated.
[66] Subject to confirmation that this will not impede interoperability or automation. Additionally, it is anticipated that the discussion and development of technical specifications will consider how a point-of-contact or other information can be incorporated.

	transaction going back to the manufacturer, as applicable.
Output of Tracing	
Requirement-Trac-011	Systems and processes for Tracing must enable the return of one of three outputs, as designated by the Initiating Entity:[67] 1. Each TI associated with the sGTIN being traced, including both the TI generated by each selling ATP and the TI received and captured by each purchasing ATP. 2. A listing of each ATP that has owned the product associated with the sGTIN being traced. 3. Identification of the last ATP known to have owned the product associated with the sGTIN being traced.
Requirement-Trac-012	With regard to the output in Requirement-Trac-011(1), the TI shall be limited to summary TI information[68] solely for the specific sGTIN(s) being traced.[69]
Requirement-Trac-013	With regard to the output in Requirement-Trac-011 and 012, the TI (or a subset of the TI elements) collected shall include both the TI provided by the seller in a given transaction and the TI received and maintained by the purchaser in that transaction, and both the selling ATP and purchasing ATP shall provide their respective information.[70]
Requirement-Trac-014	Systems and processes for Tracing shall not require an ATP to speak to or bear responsibility for the content of any TI other than the TI that ATP received at the time of purchase and the TI it provided at the time of sale.[71]
Requirement-Trac-015	A request for Tracing and the outputs of systems and processes for Tracing shall be treated as confidential by all ATPs, and (i) shall only be used for purposes of supporting a suspect or illegitimate product investigation or recall, as relevant, and (ii) shall only be made available to individuals within the ATP who have a specific need to for the information.

[67] Stated differently, the Initiating Entity should have the ability to designate which of the three types of output it is seeking. This does not reflect any presumption about how this output is gathered or who gathers the output; it simply defines the output of whatever process is ultimately agreed to. Here again it is important to note that this requirement must be read in conjunction with other requirements, particularly Requirements-Trac-013 and -014.

[68] For example, if part of the TI is incorporated into an invoice, the response information shall be limited to only those pieces of information that are statutorily defined TI elements.

[69] For example, if the sGTIN being traced was part of a sale of 100 units, the TI shall be limited to that one individual sGTIN, not TI for all sGTINs in that sale.

[70] For example, assume only one transaction has occurred—a sale from manufacturer to wholesale distributor. The manufacturer must provide the relevant information associated with the sale of the product, and the wholesale distributor must provide the corresponding information associated with the purchase of the product. Neither the manufacturer nor the wholesale distributor shall be individually responsible for the information associated with both sides of the transaction.

[71] Even if an ATP facilitates the gathering of additional information from other ATPs, it should not be *responsible* for that other ATP's TI.

Speed of Tracing	
Requirement-Trac-016	The systems and processes for Tracing shall be configurable to enable Responding ATPs the optionality to respond in a rapid automated manner or to manually review the request and respond within one business day.[72]
Audit/Testing	
Requirement-Trac-017	Systems and processes for Tracing-Suspect, Tracing-Illegitimate, and Tracing-Recall must allow tracing for audit or testing purposes. When performed for testing or audit purposes, the systems and process must clearly identify for all Responding ATPs that the tracing process is being performed for the purpose of audit or testing.

Requirements and Recommendations to Support Credentialing and Trading Partner Authentication

To support interoperable verification and tracing, users of an interoperable system must demonstrate they (or if a solution provider, the clients on behalf of which they are acting) are "authorized"[73] as defined in the FD&C Act 581(2). Unlike TI and TS exchange, which occurs between direct trading partners, interoperable verification and tracing requests may be initiated by any trading partner within the ecosystem and therefore may necessitate connectivity and information sharing between entities in the supply chain that do not otherwise conduct business with one another. As such, trading partners implementing the PDG blueprint will be required to be credentialed as a way of demonstrating their authorized status and identity in an efficient, trusted manner.[74] It is important to note that credentialing of trading partners will occur at the corporate-trading partner level. Under the DSCSA, any affiliate (subsidiary, parent, sister, or other jointly owned entity) of a trading partner is treated as one joint trading partner. As such, only one credential is required per trading partner (including affiliates).[75]

The credential(s)[76] PDG members receive must ensure the organization is both authorized (as statutorily defined) and identity proofed. We will describe each of these requirements separately as follows:

1. An ATP Credential: An ATP Credential will ensure the organization is *authorized*, as required and defined by the DSCSA.
2. An Organizational Identity Credential: An organizational identity credential ensures the organization had been *identity proofed* by independently validating the organization is who they claim to be (i.e., each organization is uniquely identified to allow the organization to demonstrate that they are who say they are).

A trading partner that demonstrates both authorized status according to the DSCSA and identity according to PDG-defined credentialing process will be considered "credentialed" within the PDG environment. Within the PDG environment, there will be a single governance authority (the "Accreditor")[77] that will be responsible for setting the guidelines for all parties and ensuring sustained compliance with those guidelines either directly or via an approved third party. The Accreditor would ensure that the issuers of each credential (the "Accredited Credential Issuer") adhere to standardized and minimum criteria for validation of "ATP status"

[72] As discussion of the technical specifications to meet this requirement advances, it is recommended that stakeholders consider whether it is feasible to respond more rapidly in certain use cases (*e.g.*, a recall or an output of the list of owners) versus other use cases (*e.g.*, an illegitimate product). It is anticipated that this requirement will evolve as stakeholders continue to evaluate options and solutions and as FDA guidance provides directional input.
[73] The term "authorized" is further defined in the glossary.
[74] The term "credentialed" is further defined in the glossary.
[75] *See* Food Drug & Cosmetic Act (FDCA) § 581(1), 581(24)(B)(i).
[76] It remains to be determined whether the demonstration of authorized status and identity will occur through one single credential that shows both or whether separate credentials are needed to demonstrate authorized status and identity, respectively. This will be addressed through PDG's ongoing discussions and future chapters of this document.
[77] The term "Accreditor(s)" is further defined in the glossary.

(as statutorily defined) or "Identity." Individual trading partners will acquire their credentials from an Accredited Credential Issuer.

Authorized Trading Partner (ATP) Status	
Manufacturers	
Requirement-Cred-001	The Accreditor must ensure that an Accredited Credential Issuer issues credentials that allow a trading partner to: 1. Confirm the authorized status of a manufacturer as part of the systems and processes for tracing; and 2. Confirm the authorized status of a manufacturer as part of the systems and processes for verification. The Accreditor must also ensure that an Accredited Credential Issuer, as a condition of issuing such credentials: 1. Uses the FDA's establishment registration database to confirm registered status of the manufacturer; and 2. Confirms that, if the manufacturer has multiple registered establishments, they will have at least one current valid registration for a registered packaging site.
Repackagers	
Requirement-Cred-002	The Accreditor must ensure that an Accredited Credential Issuer issues credentials that allow a trading partner to: 1. Confirm the authorized status of a repackager as part of the systems and processes for tracing; and 2. Confirm the authorized status of a repackager as part of the systems and processes for verification. The Accreditor must also ensure that an Accredited Credential Issuer, as a condition of issuing such credentials: 1. Uses the FDA's establishment registration database to confirm the current valid registered status of the repackager.
Virtual manufacturers[78]	
Requirement-Cred-003	The Accreditor must ensure that an Accredited Credential Issuer issues credentials that allow a trading partner to: 1. Confirm the authorized status of a virtual manufacturer as part of the systems and processes for tracing; and 2. Confirm the authorized status of a virtual manufacturer as part of the systems and processes for verification. The Accreditor must ensure that an Accredited Credential Issuer, as a condition of issuing such credentials: 1. Confirms/validates the product labeler code or obtain clear evidence that the manufacturer holds an NDA, ANDA, or BLA for a product;and 2. Confirms/validates that a CMO[79] or CLP[80] used by the

[78] The term "virtual manufacturer(s)" is further defined in the glossary.
[79] The term "Contract Manufacturing Organization (CMO)" is further defined in the glossary.
[80] The term "Co-Licensed Partner (CLP)" is further defined in the glossary.

	virtual manufacturer to manufacture at least one product has a valid registration in accordance with Sec. 510 of the FDCA.[81]
Wholesale Distributors	
Requirement-Cred-004	The Accreditor must ensure that an Accredited Credential Issuer issues credentials that allow a trading partner to: 1. Confirm the authorized status of a wholesale distributor as part of the systems and processes for tracing; and 2. Confirm the authorized status of a wholesale distributor as part of the systems and processes for verification. The Accreditor must also ensure that an Accredited Credential Issuer, as a condition of issuing such credentials: 1. Uses a database or similar source of relevant licensure information operated and maintained directly by a State licensing authority (e.g., a State Board of Pharmacy) to confirm licensure of the wholesale distributor;[82] 2. Confirms the wholesale distributor is registered with FDA's self-reported database[83], as required by DSCSA; and 3. With regard to tracing and verification, if a wholesale distributor is licensed[84] in multiple states, confirms current valid licensure in at least one state,
Dispensers	
Requirement-Cred-005	The Accreditor must ensure that an Accredited Credential Issuer issues credentials that allow a trading partner to: 1. Confirm the authorized status of a dispenser as part of the systems and processes for tracing; and 2. Confirm the authorized status of a dispenser as part of the systems and processes for verification. The Accreditor must also ensure that an Accredited Credential Issuer, as a condition of issuing such credentials: 1. Uses a database or similar source of relevant licensure information operated and maintained directly by a State licensing authority (e.g., a State Board of Pharmacy) to confirm valid licensure as a dispenser; 2. With regard to tracing and verification, if a dispenser is licensed in multiple states, confirms current valid licensure in at least one state.
Requirement-Cred-006	There should be a robust exceptions handling process for specific distribution or dispensing sites that are either permanently or temporarily not authorized.
Audit Trail	
Requirement-Cred-007	An Accredited Credential Issuer shall have systems and processes in place to demonstrate and prove the orderly implementation of the requirements as specified by Req-Cred-001 – Req-Cred-006 and

[81] This information will be provided to the Accredited Credential Issuer but the details (e.g., *who* the CMO or CLP is) should be held strictly confidential and should not be transparent to other trading partners through credentialing.
[82] The self-reported FDA database of wholesale distributor licensure information is not an acceptable alternative to a state licensure database.
[83] Accessible here: https://www.accessdata.fda.gov/scripts/cder/wdd3plreporting/index.cfm
[84] The term "licensed" is further defined in the glossary.

	appropriately secure management of the information required to carry out such requirements. Such demonstration and proof includes: a records maintained to demonstrate conformance to the PDS Blueprint requirements, the source documentation utilized to validate authorized status, including any changes to source documentation (e.g., renewed license, revoked license), and a record of modifications, if any, that are made to the record of a trading partner's authorized status (e.g., grace period exemptions). This information shall be maintained in a manner that would allow for periodic and/or impromptu inspections.
Validation of ATP Credential Source Documentation	
Requirement-Cred-008	State regulators and FDA may develop systems to push updates to license and registration data. Once available, PDG may set governance rules for use and timetable for implementation.
Requirement-Cred-009	For credentialing source documentation that originates in a state, or with FDA, where the regulator has implemented systems and processes to push updates to the Accredited Credential Issuer, PDG may set governance rules for using the system by credential issuers and a timetable for implementation.
Requirement-Cred-010	For credentialing source documentation that originates in a state, or with FDA, where the regulator has not implemented systems and processes to push updates, an Accredited Credential Issuer shall verify authorized status at least weekly and upon expiry of a current license; provided however, if a state updates its externally accessible system of record less frequently than weekly, the Accredited Credential Issuer shall verify authorized status as frequently as the state database is updated (e.g., if a state only updates their database month, the check can occur monthly) and upon expiry of a current license.
Requirement-Cred-011	If an Accredited Credential Issuer learns that the conditions of the credential are no longer met (e.g., a license has been lost), either due to a pushed notification or confirmation by the Accredited Credential Issuer, the credential shall reflect this change within 4 hours.
Requirement-Cred-012	Once an Accredited Credential Issuer has validated the evidence proving ATP status, the Accredited Credential Issuer will issue a valid and secure technical mechanism to prove and verify the ATP status of the organization. Such technical mechanism shall be interoperable with all other technical mechanisms within the PDG ecosystem.
Requirement-Cred-013	The technical mechanism in Requirement-Cred-012 shall accommodate proxy or delegated use as designated by the credentialed entity.
Organizational Identity	
Requirement-Cred-014	The Accreditor must ensure that an Accredited Credential Issuer, as a condition of issuing an organization identity

	credential, conforms to section 4.2 General Requirements for Identity Proofing of The National Institute of Standards and Technology (NIST) SP800-63A and meets Section 4.4.1.2 Identity Assurance Level 2 (IAL2) Evidence Collection Requirements of NIST when performing identity proofing. IMPORTANT NOTE: Simply collecting documents or identification numbers does not constitute identity proofing. Due diligence is required to thoroughly validate the collected documents and identification numbers. • The full set of standards can be found in Section 2 of NIST Special Publication 800-63A. • Core concepts and application of NIST IAL2 for DSCSA can be found in Sections 3-4 of the Open Credential Initiative (OCI) Credential Issuer Conformance Criteria. According to Section 4.4.1 of NIST Special Publication 800-63A, IAL2 proofing requirements requires that an Accredited Credential Issuer collects sufficient evidence to prove the: • Existence of the Organization; • Identity of the Organization; • Identity of the Organization's Representative; and • Authority of the Representative to act on behalf of that Organization. Section 4.4.1.2 (IAL2 Evidence Collection Requirements) of NIST Special Publication 800-63A states: The Credential Issuer SHALL collect the following from the applicant: • One piece of SUPERIOR or STRONG evidence IF the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence AND the Accredited Credential Issuer validates the evidence directly with the issuing source; OR • Two pieces of STRONG evidence; OR • One piece of STRONG evidence plus two pieces of FAIR evidence. 1. The above rules apply to both the Organization and its Representative.
Requirement-Cred-015	Once an Accredited Credential Issuer has confirmed an organization's identity and issued an active organizational identity credential, there is not a need to verify the identity a second time. If there is a need for the organizational identity credential to be renewed for security purposes or other reasons, that will be determined by the Accredited Credential Issuer.
Requirement-Cred-016	If an Accredited Credential Issuer has evidence that one (1) or more of the documents or identifiers identified in Req-Cred-014 and Req-Cred-015 are not valid, the Accredited Credential Issuer will not issue an identity credential.

Requirement-Cred-017	Once an Accredited Credential Issuer has validated the evidence proving organizational identity, the Accredited Credential Issuer will issue a valid and secure technical mechanism to prove and verify the identity of the organization. Such technical mechanism shall be interoperable with all other technical mechanisms within the PDG ecosystem.
Requirement-Cred-018	The technical mechanism in Requirement-Cred-017 shall accommodate proxy or delegated use as designated by the credentialed entity.
Audit Trail	
Requirement-Cred-019	An Accredited Credential Issuer shall have systems and processes in place to demonstrate and prove the orderly implementation of the requirements as specified by Req-Cred-014 – Req-Cred-017 and appropriately secure management of the information required to carry out such requirements. Such demonstration and proof includes: a record of each confirmation of authorized status (i.e., a valid Accredited Credential Issuer-issued technology mechanism in combination with the organization's technology mechanism), the source documentation utilized to validate authorized status, including any changes to source documentation, and a record of modifications, if any, that are made to the record of a trading partner's authorized status (e.g., mergers, acquisitions). This information shall be maintained in a manner that would allow for periodic and/or impromptu inspections.

Change Control

Date of Change	Section	Description of Change	Approved By
7/7/2021	Ch.1; Requirement-Ser-021	Added full spelling of "sGTIN"	PDG Board of Directors
7/7/2021	Interoperable Tracing Intro	Added new FN55	PDG Board of Directors
7/7/2021	Ch. 1; Requirement-Cred-001 through -005	Revised to clarify that credentials must enable confirmation of ATP status as part of the systems and processes for tracing and verification in both requestor and responder scenarios	PDG Board of Directors
Version 1.1			
7/15/2022	Ch. 1: Requirement-Cred-001, 002, 003, 004, 005, 007, 008, 009, 010, and 014	Revised requirements	PDG General Members
7/15/2022	Ch. 1: Requirement-Ser-023	Added new FN26	PDG General Members
Version 1.2			
4/12/2023	Ch. 1: Requirement-Trac-010	Minor spelling correction	PDG Board of Directors
Version 1.3			
		No Changes in this version	