Specifications to Implement a Technology Architecture for Enabling Interoperable Food Traceability

The GFTC greatly appreciates the contributions to this document provided by the members of the Technology Architecture Working Group.

Editors: Tejas Bhatt and Martin Gooch

Table of Contents

Reference for citation:

Bhatt T, Gooch M, editors. 2017. Specifications to implement a technology architecture for enabling interoperable food traceability. Chicago: Global Food Traceability Center, Institute of Food Technologists. Available from: http://www.ift.org/gftc/resources.aspx.

I. Executive Summary

The seafood industry is increasingly competitive, global, and complex. The ability to proactively manage risks, reduce costs, and increase revenue rests on the effective sharing of data and information between businesses operating along the supply chain and between businesses and other stakeholders. Verifying the accuracy and rigor of data exchanged within and between businesses relies on the existence of effective interoperable information systems. Effective interoperability necessitates the sharing of a common technology architecture (blueprint) framework among the systems used by businesses operating along the value chain. An interoperable traceability technology architecture is a collection of interrelated specifications, standards, and practices for hardware, software, and communications interfaces which, together with core services, operate in service of a common goal. The technology blueprint designed and described here is based on a distributed peer-to-peer networked database architecture for enabling interoperable traceability. Because there is no central database, distributed peer-to-peer networked databases offer a number of advantages—including scalability and robustness—in comparison to alternative designs.

Technology architectures are developed by engaging industry stakeholders in a purposeful dialogue about why the architecture is required, and what it means for industry in terms of benefits and opportunities, as well as the components and specifications required to translate a conceptual design into a solution that meets the needs of industry and other stakeholders. This specifications document resulted from the establishment by the Institute of Food Technologists' (IFT) Global Food Traceability Center (GFTC) of a working group to advance the concept of a technology architecture suited to enabling interoperable traceability in seafood, and subsequent initiation of architecture design through development of technical specifications. The working group recognizes that the initial ("strawmodel") architectural model and components described in this document will develop over time with further vetting by industry stakeholders, including businesses and third-party solution providers, and peer-review.

This document reflects that the main idea of traceability is to record relevant information (referred to as KDEs [key data elements]) associated with the physical goods ("traceable entities") as they move through specific steps (CTEs [critical tracking events]) in the supply chain, and to make that relevant information available in a timely fashion to achieve specific business objectives. Stated another way, KDEs are attributes describing CTEs which are descriptions of physical events that occur in a product's lifecycle. KDEs and CTEs also relate to product lifecycles. Thus, KDEs and CTEs are essential data for an effective interoperable traceability technology architecture. As seafood supply chains become more global and complex, and consumers demand more variety, operations include the aggregation of similar and heterogeneous products from different sources and the manufacture of multiple ingredients into processed products. This leads to the need to track multiple lots and may result in an enormous amount of data. Therefore the architecture and the components that will enable it to function must be suited to managing "big data"[1] while simultaneously providing granular insights as required.

This document begins by describing what is within and out of scope. In-scope considerations include commingling and other aggregation and segregation practices occurring within the supply chain (including transshipment) and relevance to supply chain participants from harvesters, to fishing vessels,

[1] The term big data describes extremely large sets of data that require advanced computerized capabilities to reveal trends, patterns, and associations that can be used to make informed decisions.

processors, packers, distributors, transporters, wholesalers, retailers, and government agencies. Because significant investments in traceability have already been made, an incremental rather than a radical approach to traceability improvement is recommended. Out-of-scope considerations include relevance of the architecture to consumers, specific CTEs and KDEs, cost–benefit analysis, and governance arrangements.

The document also describes experiences and challenges that guided the evolution of the strawmodel technology architecture along with the identification of process and technology capabilities required to achieve interoperable seafood traceability. These capabilities reflect principles that were found to be critical to enabling full-chain interoperable traceability to occur, by connecting internal and external computerized traceability systems. To be effective and have long term viability for individual stakeholders as well as industry overall, the architecture must encompass technology solutions that together result in inherently flexible, customizable, and adaptable applications. Example technologies to enable the architecture to function, initial technical specifications, and potential vendors are described. This document concludes with further considerations and next steps.

II. Introduction

1. Objectives

This document is one deliverable from a project led by the Institute of Food Technologists' (IFT) Global Food Traceability Center (GFTC) to establish a common interoperable traceability technology architecture for the global food industry. In the initial phase of the project, a conceptual blueprint for a global interoperable traceability system for the seafood industry was developed, and an Issues Brief (Bhatt and others 2016) was produced that addresses enterprise-level traceability systems and provides recommendations to inform the design of an appropriate technology architecture. Other deliverables include international stakeholder engagement activities, along with the development of awareness and training materials. Throughout the project consideration is being given to the potential future role of the architecture in the global food industry per se. This document presents the detailed concept for an interoperable traceability technology architecture that will allow implementation of interoperable food traceability practices on a global scale. Additionally, this document describes the technical and functional prerequisites that are necessary for the interoperable technology architecture to accommodate the unique needs and internal practices and systems of individual firms.

The GFTC recognizes the importance of identifying and engaging all stakeholders that are important to the design of the architecture and its delivery, rollout, implementation, and effective functioning. These stakeholders include diverse public and private entities: regulators and government agencies, technology solution partners, non-government agencies, and food system sectors (that is, suppliers, producers/farmers, processors, distributors, retailers, and foodservice entities). Recognizing the need for and value of an evolving and iterative process to establish the blueprint, the GFTC continues to seek additional input from stakeholders through the publication of this document and the stakeholder engagement activities mentioned above.

2. Scope of Design Document

The initial focus of this interoperable architecture is seafood; however, consideration has been given to the utility of its application for other food sectors. It is pragmatic to consider all food commodities as potentially benefiting from such an interoperable architecture, given the supply chain complexities within the seafood industry, the myriad stakeholders involved in getting foods from point of harvest or catch to the point of consumption, and the fact that seafood is aggregated with other foods at points along the supply chain, particularly in manufacturing, retail, and foodservice (Sterling and others 2015). In fact, some other initiatives, for example the one being led by the Consumer Goods Forum (a global network of more than 400 retailers, manufacturers, service providers, and other stakeholders across 70 countries) go beyond food, and look at enabling interoperable traceability across non-food commodity sectors as well. This section summarizes aspects of the traceability architecture that are within and out of scope for the purpose of this specifications and design document.

2.1 In Scope

We have given consideration to the following in the design of the interoperable architecture concept. While many of the issues surrounding the development of effective interoperable traceability systems described in this document are applicable to all foods, those appearing below pertain to issues specific to seafood commodities and the seafood industry:

- Commingling and other aggregation and segregation practices within the supply chain (including transshipment)
- Relevance to supply chain participants, from harvesters, to fishing vessels, processors, packers, distributors, transporters, wholesales, and retailers
- Relevance to governmental agencies as data providers and data consumers within the architecture
- Recognition that significant investments in traceability have already been made and an incremental approach to improvement may be needed, considering current traceability systems available and/or in use around the world
- Recognition of an iterative development methodology to improve the design through a thorough successive vetting and peer-review

2.2 Out of Scope

The following considerations are out of scope for the purpose of this document, because they are the primary focus of other research and/or initiatives:

- Relevance of the architecture to the consumer
- Specific CTEs and KDEs required for interoperability (in an attempt to build a data-agnostic framework)
- Cost – benefit analysis
- Governance of traceability practices (such as non-data-related business practices)
- Implementation guidelines
- Design documents of a theoretical nature, that may work well in theory but which would not be pragmatic enough for implementation at this time.

3. Approach to Advancing the Architecture Concept

To advance the concept for the traceability technology architecture and initiate its design through technical specifications, the GFTC engaged technical experts with expertise in seafood industry processes and systems, traceability systems, technology solutions and third-party solution providers (TPSPs), computer engineering, and interoperability. These experts have affiliations with technology, consulting, analytical/laboratory testing, seafood manufacturing, seafood industry trade associations, international non-profit and non-governmental organizations relating to conservation, sustainability, sustainable fishing, certification, and identification. The experts were part of a working group that deliberated on: (1) guiding and informing the development of the conceptualized interoperable traceability technology architecture, and (2) proposing pragmatic solutions to issues to achieve system and technical specifications that would enable effective traceability throughout the entire supply chain. The group met 5 times for discussion and deliberation of various considerations and subsequently contributed to the drafting and production of this document. Working group members and contributors are identified in Acknowledgements.

III. Architecture Framework

4. Overview: The Concept

An interoperable traceability technology architecture is a collection of interrelated specifications, standards and practices for hardware, software, and communications interfaces which, together with core services, operate in service of a common goal. The technology blueprint being designed and described here is based on a distributed peer-to-peer networked database architecture.

The architecture is designed for multiple uses and constructed on a common set of requirements, analogous to telecommunications system requirements. The architecture is intended to be sufficiently flexible to embrace the diversity of business systems that are in use and independent of the kind of information system used by individual organizations. The architecture is intended to function using existing business systems and transactional data through publicly available standardized protocols that provide secure access to relevant, reliable, and readily accessible traceability information.

As in telecommunications and the financial services, automotive, produce, pharmaceutical, and other industries, interoperability between TPSPs allows users to communicate or have access to information and services seamlessly. This is accomplished through global governance, agreed-upon technical specifications and standards, a legal framework, and agreed-upon commercial terms. While food traceability has its own unique characteristics and complexities, the approach to interoperability should contain the same elements.

4.1 Third-Party Service Provider Concept

A partial strawmodel interoperability architecture, from a TPSP perspective, is shown in Fig. 1. For reasons described below, the architecture has API (application programming interface) for interoperability with other TPSPs, including 'Virtual Lock Box' capabilities. This enables Discovery Service (query and response mechanisms, including data mining capabilities), and Automated Query & Response Portal capabilities.

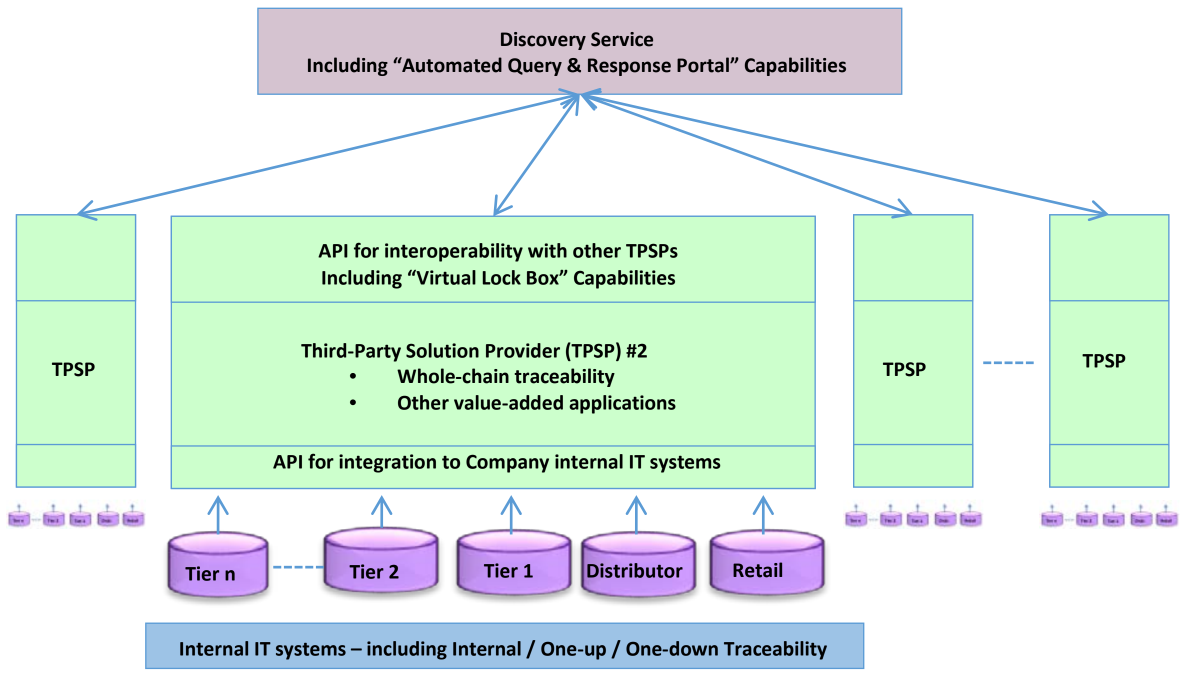

Figure 1 – Partial interoperability architecture strawmodel, from a third-party solution provider perspective (Kittelsen 2016).

Key aspects of the architecture concept are:

- Individual businesses have internal systems for internal traceability, including "one-up, one-down" recordkeeping. These systems, typically produced by a TPSP, may incorporate global standards or have proprietary specifications, or a mixture of both.
- For electronic external traceability, that is, sharing agreed-upon information between trading partners, a business would typically use an appropriate TPSP. If there is interoperability between TPSPs, an individual business should be able to share traceability information seamlessly with trading partners who may subscribe to different TPSPs.
- Individual TPSPs typically focus on specific market segments (that is, industries such as food, financial, or pharmaceutical, in combination with supply chain sectors such as retailers and/or brand owners), offering business benefits that appeal to particular needs (such as risk reduction, supply chain efficiency, brand protection, and strengthened sustainability).
- The suitability of TPSPs for performing a specific role/task and the rigor of their subsequent work may be subject to certification by third-party auditors who are not employed by the TPSP or their client. TPSP audits are a particularly common feature of electronic technology initiatives performed in the finance industry (FFEIC 2012).

4.2 Architectural Strawmodel

Based on the insights discussed above and input from technology and traceability experts from around the world, the strawmodel initially chosen as the technology architecture for enabling interoperable seafood traceability is shown in Fig. 2. This model will be further described and developed over time with further vetting and peer-review. The strawmodel's design evolved from the conceptual design shown in Fig. 1, following the recognition that it could not adequately address challenges voiced by stakeholders given the complexities intrinsic to enabling effective traceability and data security concerns within the food sector. For example, given the large volumes of food that flow through the global food system, an exponentially larger amount of data would need to flow through the traceability architecture for tracking purposes. Therefore, with the goal of architecture scalability and robustness, it was decided that there could be no central database (whether physically in a data center or "in the cloud") to contain all the traceability data from the global food system. Instead, data will be housed in a peer-to-peer distributed networked database with access provided to queries according to pre-agreed controls in place.

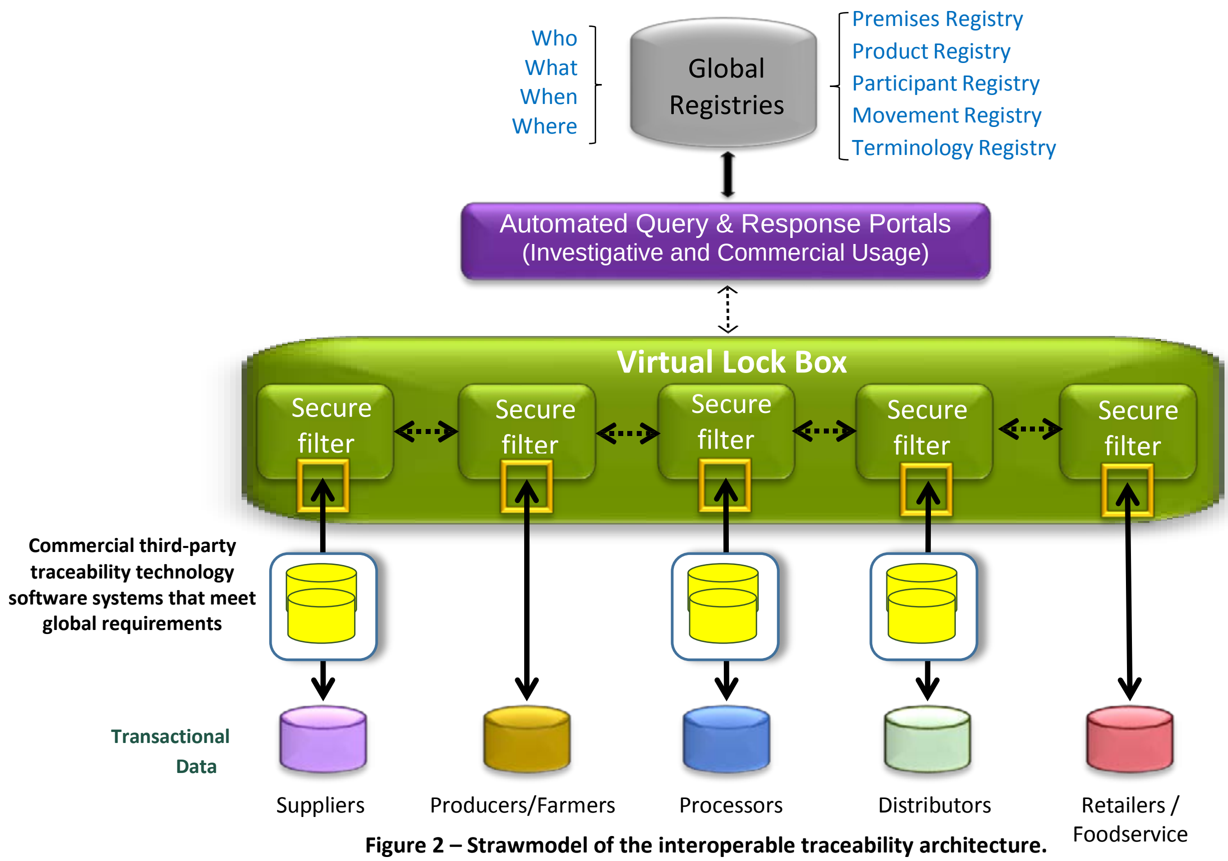

Figure 2 – Strawmodel of the interoperable traceability architecture.

This design addresses a common concern of the industry—that of data ownership and security—when participating in an interoperable traceability architecture. By enabling a distributed system, industry stakeholders and government agencies can maintain control of their own data within their own internal database systems (either internally owned or contracted to a TPSP). At the same time, certain types of KDEs and certain CTEs can be recognized as data that need to be shared or made accessible for the purpose of enabling syntactic and semantic interoperability. This strawmodel proposes isolating these “linking” KDEs into a virtual lock box, further protecting the business confidential and transactional KDEs that reside in internal systems.

The virtual lock box concept is built on the feature that the data are called only as needed and are not stored locally, and is responsible for enabling access control and for receiving, interpreting, and responding to queries from supply chain partners and regulatory agencies. While the strawmodel illustrates a single query and response model within the architecture, due to the peer-to-peer distributed database design, it is more likely that the implementation of such a portal would evolve into a distributed query and response portal as well. For example, the U.S. National Oceanic and Atmospheric Administration (NOAA) is proposing their own query and response portal through the establishment of the seafood traceability program for the purpose of combating Illegal, Unreported, and Unregulated (IUU) fishing and seafood fraud at the time of importation (NOAA 2015, 2016). Similar parallel portals could be built by: an individual company to query its multiple locations/facilities, a participant in the supply chain to query its supply and customers, a supply chain to query the participating stakeholders, or other countries or regions. Finally, the strawmodel also recognizes the need for global registries required by the architecture for verification of reliable data and standardization of data. This is covered in greater detail later in this document.

IV. Enabling Implementation

The remainder of this document discusses factors that are important to enabling the effective implementation of the technology architecture for interoperable traceability. Factors discussed include the standards for identification, technology, and communication that are required to enable API communications and Virtual Lock applications, as well as guide the development of standardized APIs. The information begins with details of principles that will determine the successful application of the technology architecture. Following this are specific examples of potential technical solutions.

5. Principles and Essential Elements in Architecture Design and Interoperability

Presented below are the principles that must exist for electronic interoperability to occur for traceability in the seafood industry. Gupta (2008) describes a principle as a fundamental truth that provides a simple description of what is required to execute functions and solutions to problems in systems that are themselves complex. The principles guide designers in understanding the behavioral characteristics that a system must have to achieve a specific purpose, therefore applying to any food, not just seafood. The principles encompass those previously developed to ensure that computerized systems operate effectively and efficiently, such as those described by Ross and others (1975) and Reed (2006).

The principles are categorized into “structural principles,” “operational principles,” and “integrative principles.” Structural principles are fundamental and must exist to ensure that the interoperability architecture remains viable through continual evolution in line with industry requirements. Operational principles describe the elements which determine the functions and capabilities of systems. Integrative principles enable businesses and the supply/value chains in which they operate to use interoperability in the creation of value. While operational and integrative principles must exist, their exact nature will be determined by users’ needs and the environment in which they operate. A diagram illustrating how the 3 sets of principles relate to each other in enabling interoperability is shown in Fig. 3.

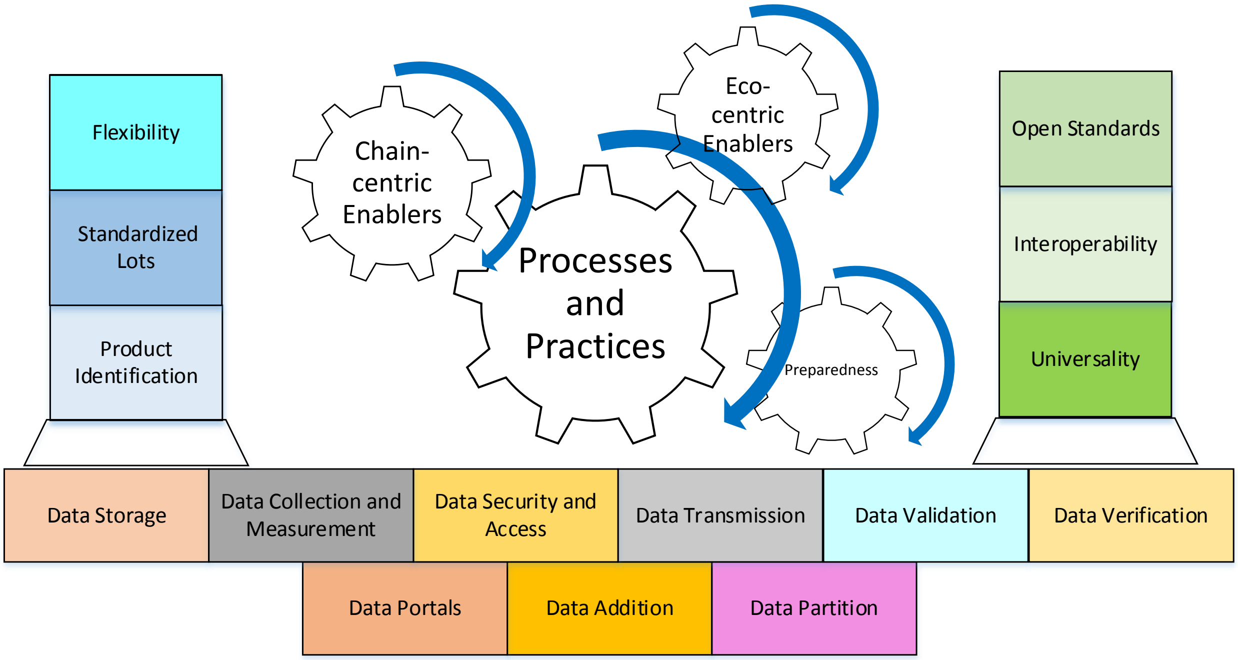

Figure 3 – Interrelated principles for enabling interoperable seafood traceability.

5.1 Structural Principles

Interoperability

Interoperable architecture must have the capacity to support "syntactic" and "semantic" interoperability at the broadest levels so that computer systems can be used to exchange data and subsequently present that data to allow it to be communicated and understood by all users. Unless the architecture supports "syntactic" and "semantic" interoperability it will not possess the extensibility capabilities required to ensure its long-term viability by enabling new functions to be added.

Universality

Internal traceability systems possess the ability to autonomously meet the unique needs of thousands of individual companies. Internal traceability systems must also have interoperable capacity, so that inputs from external systems and outputs from internal systems can be suitably connected via the technology architecture to the various traceability support systems that extend across tens of thousands of supply chains.

Flexibility

To prevent users from being restrained by excessive rules, protocols, and inefficiencies, the technology architecture must be inherently adaptable to meet the needs and practices of a diverse range of individual firms, supply/value chains, private contracts, and regulatory regimes. This can be achieved, for example, by requiring that structures and functionalities be configurable to meet diverse needs of users whose information and traceability requirements vary across supply chains and change over time.

Open Standards

The architecture's success and flexibility will depend on industry agreement on a base of standards that define species, measurements, CTEs and KDEs, and key protocols, aided by a common ontology. For example, standardized protocols for data measurement and data sharing will be essential for the success and effectiveness of whole-chain traceability. This is typically overseen by a governance body established to oversee the process of developing new industry-driven schema.

Standardized Lots

The architecture will need to allow for standardized lots that may be diverse in their specific size and format, although readily and accurately communicable between trading partners/stakeholders. Ensuring the consistent expression of what constitutes a lot is critical to interoperability because the seafood industry does not organize production output or data into simple or consistent standard formats, and the characteristics of both products and lots are often transformed as products move along supply chains.

Product Identification

The architecture must allow for human- and machine-readable codes associated with each product and location. The codes could be comprised of global identifiers that uniquely distinguish product type, and lot numbers that pinpoint product at a sufficiently granular level (for example, dates, vessel, production facility, and so on). The original harvest lot must be identified and linked to all other "lot" or "process/batch" numbers generated during supply chain activities.

5.2 Operational Principles

Data Addition

Within the architecture, all data generated by each node in the supply chain must be linked. When a new lot number is assigned, previous lot numbers will be linked to the new lot. The purpose of this linking is that traceability must exist for the product throughout its entire lifecycle.

Data Portals

The architectural design includes portals for receiving, transmitting, and accessing (querying) data in granular or aggregated form, depending on the system user's role, access rights, and relationship to the data. Intermittent access to singular packets of data or wider capabilities, such as continuous search options, will be controlled and tailored according to individual firm and supply chain needs.

Data Partition

The architecture will function to minimize data-siloing in order to provide access to product data via the architecture's portals. Access to data will be conditional on proper permissions, and high-level security.

Data Storage

The architecture must be designed to minimize the need to store data outside the firm. The principle is to store all data as close as possible to where it was gathered and provide visibility of the data instantaneously via secure portals.

Data Transmission

The architecture is designed to transmit data electronically, as allowed by required permissions. Unique identifiers would be transmitted with both the data and the product. Data can be transmitted via software and hardware arrangements that best meet the strategic needs of individual businesses and supply chains, ensuring their practical application in different conditions.

Data Security and Access

The architectural framework must be secure, to protect personal privacy along with the intellectual property and security of individual companies. User permission to access data would be granted by each firm via predefined arrangements granted to individual users of data. Different classes of data may have different permission requirements.

Data Collection and Measurement

The architecture requires that stakeholders define KDEs and implement standardized measures to monitor performance and validate authenticity. Data collection would be done by individual companies, using a variety of techniques (for example, paper, electronic sensors, and scanners, and so forth). When required, the means must exist to convert manually-recorded data into electronic form.

Data Validation

The architecture must be able to identify key missing data in the transmission process, thereby ensuring compliance with established common standards, specifications, and protocols. Validation is also required to prevent erroneous data from entering the system. Data validation will be achieved by the architecture providing the ability to transmit third-party authenticators for firm-level data or other firm-level validation information. Examples of firm-level data validation methods include identifiers denoting user location and field constraints programmed into software applications.

Data Verification

The architecture should be able to verify the authenticity of the data flowing through the systems. This requires the identification of authoritative sources of data (for example, global registries) as well as certifications and verification protocols using first, second, and third-party audits.

5.3 Integrative Principles

Preparedness

The architecture design must encompass sufficient tools and instruction so that firms can select options (for example, self-diagnostic tools) that best suit their needs, so that they can accurately assess their traceability needs and produce realistic outcomes given current inter-firm relationships/capabilities. This will ensure viable returns on investment and the minimal level of expenditures required to achieve the firm's or supply chain's objectives.

Processes and Practices

The architecture's design requires a clear understanding of processes that are core to information systems used for both internal and external traceability, as well as the range of practices that can be employed in designing a global architecture. The processes that define information technology and its use for traceability are foundational and relatively few in number. The practices that firms use to record, store, analyze, and distribute product information will vary significantly and according to the stakeholders' roles in the supply chain, scale of operations, and technical capabilities. The selected practices that bring these processes to life must efficiently align the processes that are external to individual firms, as well as support the alignment of these processes within the firm.

Eco-centric Enabling Conditions

The architecture must recognize that 'enabling conditions' for traceability, including technological, educational, and governance infrastructures, are at minimal levels across many regions of the globe. A global architecture must contend with these holistically in order to support a technologically diverse set of users.

Chain-centric Enabling Conditions

The architecture must recognize the diverse and dynamic nature of inter-firm relationships (for example, "fragmented," "cooperative," "coordinated," or "collaborative").[2] This enables firms to have choices appropriate to the current state of their system, and then easily extend these choices as their collaborative relationships strengthen. While traceability systems typically begin by addressing compliance requirements (for example, safety or sustainability), their purpose often evolves to address wider ranging needs (for example, fraud, waste, and production or marketing efficiencies).

[2] For a description of characteristics pertaining to the 4 types of supply/value chain and the use of traceability for commercial purposes, see Project to Develop and Interoperable Seafood Traceability Technology Architecture: Issues Brief (Bhatt and others 2016).

6. Identification Standards

A key activity of traceability is to record relevant information (referred to as KDEs) associated with the physical goods (traceable entities) as they move through specific steps (CTEs) in the supply chain, and to make the relevant information available in a timely fashion to achieve specific business objectives. Stated another way, KDEs are attributes describing CTEs, which are descriptions of physical events supporting a product's lifecycle. Thus, KDEs and CTEs are essential data for an effective interoperable traceability technology architecture. Therefore, the main elements of traceability are the standardized definitions and identification schemes for:

- companies
- locations ("premises")
- traceable entities (external and internal)
- CTEs
- KDEs

6.1 Identification Challenges

The nature of modern seafood supply chains creates numerous challenges that must be acknowledged in the development of standards for capturing the data required to enable traceability (Mavity and others 2012). The process of harvesting and processing seafood is rarely linear. The days of one fish sold whole, headed and gutted, or frozen for the end user to further prepare are gone. The supply chain is now global and complex. As consumer markets demand more variety in larger volumes, distributors and manufacturers need to combine lots potentially from different sources. Commingling of various types and sizes of fish is a solution for efficient processing. Traceability with interoperability must accommodate this operational complexity. The array of KDEs associated with this complexity is potentially immense.

Figure 4 illustrates the basics of the water-to-table seafood system and the challenges of tracing. Seafood caught in the wild may be gathered from multiple small vessels and transshipped onto a larger aggregation vessel prior to landing. Terms use to describe large aggregation vessels include "reefer" (Bours and others 2013)[3] and "mothership" (NFI and GS1 US 2011). An example of this practice is wild pink salmon caught in U.S. waters, which may be harvested by small vessels using nets, traps, or purse seines. Fish are headed and gutted on board the reefer or at the plant and frozen into 20 kg-blocks of fish, with no segregation by harvest method (that is, gear type) or supplier. The blocks are transferred to cold storage or a refrigerated container ship and may be shipped to China for further processing during several days of production. From there, small lots may be co-mingled at the buyer level into a new single lot and shipped back to another country for secondary processing. By this point there are multiple suppliers and buyers gathering many lots of fish caught during a period of time using differing gear types.

[3] See http://www.greenpeace.org/australia/en/news/oceans/The-longline-of-suffering-and-destruction/ for the concise graphic developed into tuna catch, aggregation, and landing.

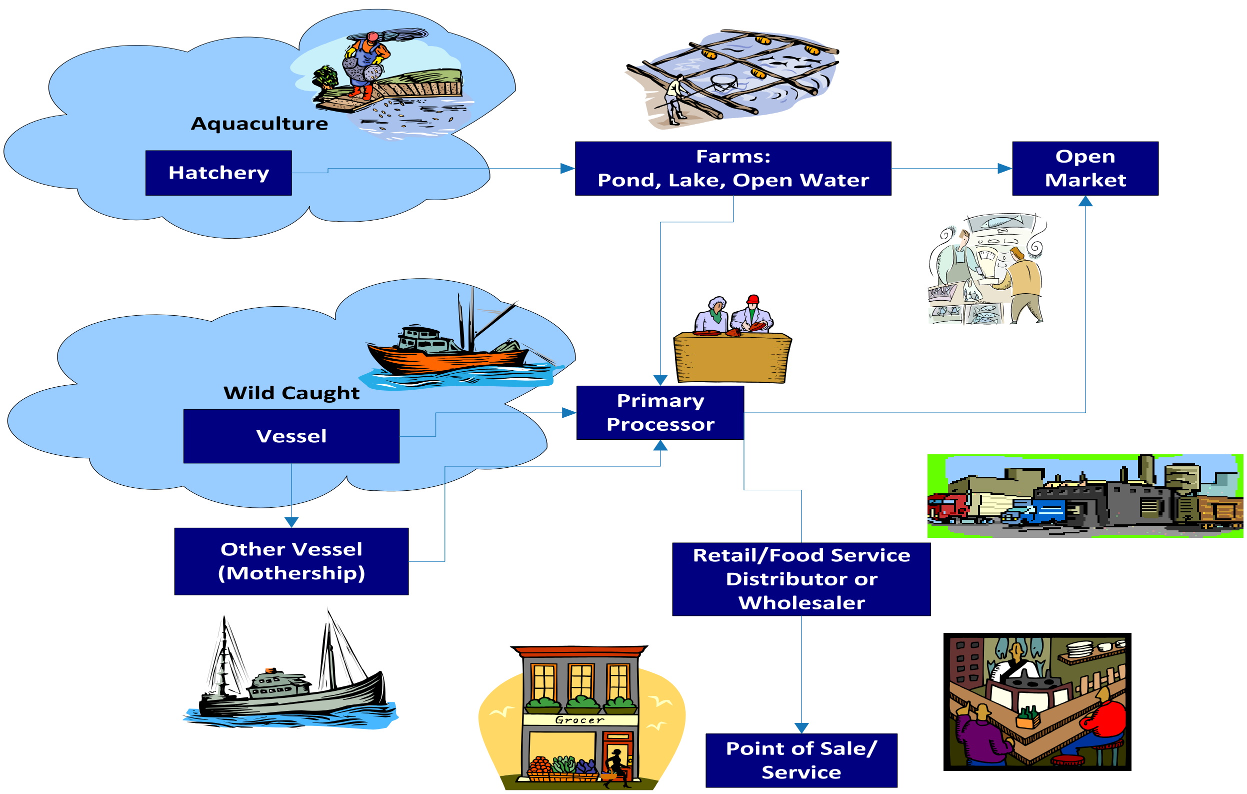

Figure 4 – Seafood supply chain (NFI and GS1 US 2011). Reprinted with permission, GS1 US; http://www.aboutseafood.com/sites/all/files/FINAL%20Seafood%20Trace%20Guide_v1.1.pdf.

Shrimp produced via aquaculture present a similar commingling challenge. Multiple ponds are required for volume requirements and efficient processing. Shrimp are sorted by size and combined to form a single code-date lot. As processing continues in the supply chain, code-date lots may be further combined. A logistical nightmare may result if the lots must be kept separate, as indicated in a theoretical scenario (Fig. 5) provided by the National Fisheries Institute (NFI 2015a). This scenario begins with 2 primary processors sorting from 2 farms each with 2 ponds. Each of the primary processors produces 2 different sizes of shrimp on separate processing lines which results in 2 separate production lots, one for each shrimp size. These 2 lots could be sold to 2 different customers, one being a secondary processor who in turn produces 2 lots of product, one of each size. NFI states that if commingling did not take place, 32 separate lots would need to be tracked (8 by each of the primary processors and 16 by the secondary processor). Given that shrimp is the top seafood choice of Americans, tracing the volume of species from water to table is a serious technical challenge (NFI 2015b).

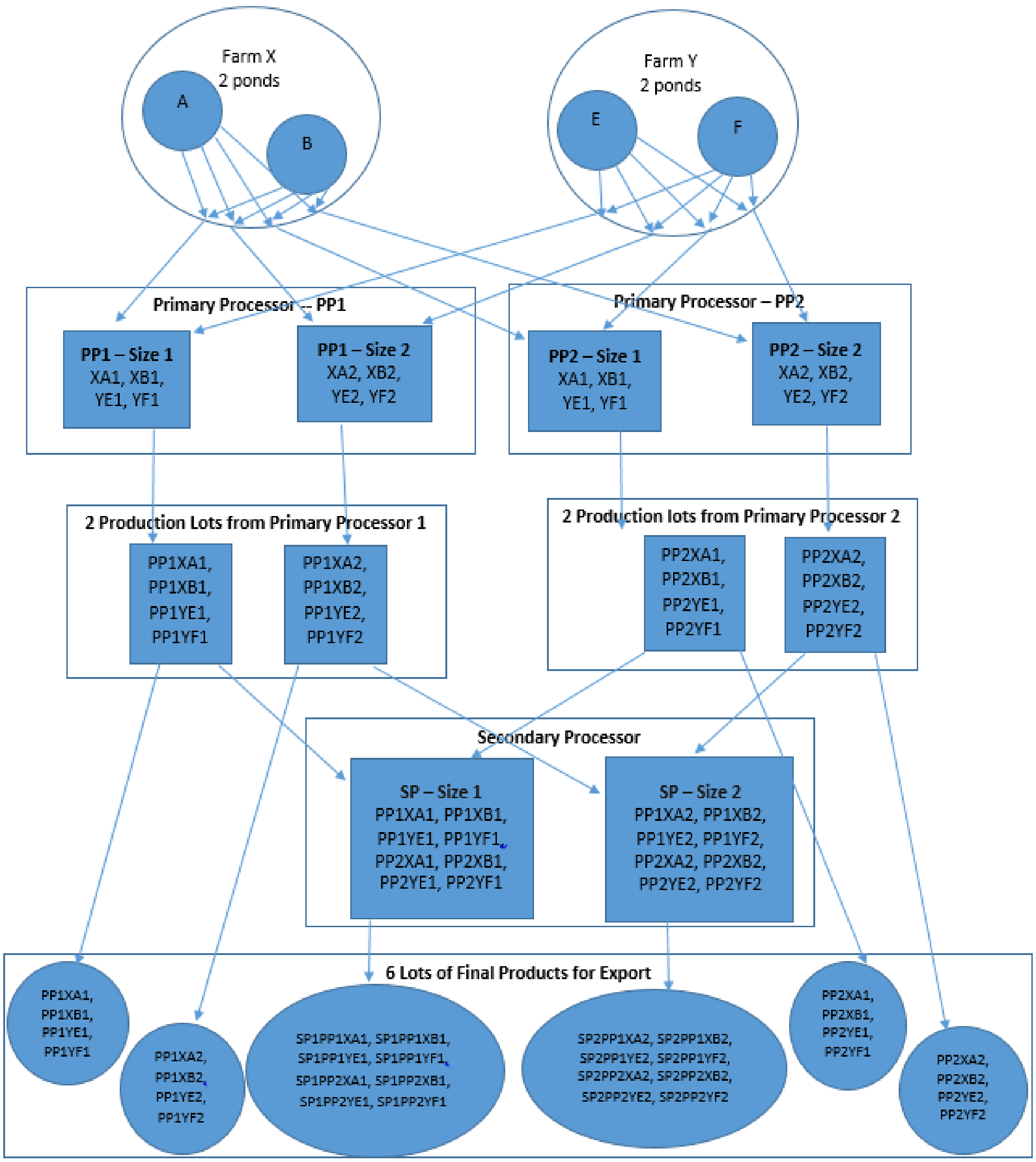

Figure 5 – Farmed shrimp scenario with commingling for line efficiencies
(NFI 2015a).

Pasteurized crabmeat is another challenge. Crabbers offload their daily harvest at a centralized landing/cooking station. In the case of blue swimming crab from Indonesia, the crabbers are artisanal fishermen whose tiny vessels are their own and are typically unregistered. The harvest from multiple crabbers are cooked and transported to the picking facility. Crabmeat will be packed into 2-3 different cans as sorted by type (for example, lump, claw, back fin), and then pasteurized.

Tuna, which are highly migratory fish, are caught by multiple registered vessels on multiple days. One fish does not equal one can of tuna fish. With albacore there are 14 size categories for processing; thus, multiple vessels are required to obtain sufficient meat for the pre-cooking step. Skipjack tuna, on the other hand, is more homogeneous in sizing, but the issue of sufficient weight for pre-cook remains.

These few examples illustrate that while there is no "one size fits all" for seafood, a standardized set of CTEs and KDEs is critical for ensuring that all data entered is true and correct, allowing an efficient mechanism for validating and verifying data, and enabling interoperability. This means that the actual CTEs and KDEs used will depend on the species being harvested, and the processes used to catch, process, and distribute the seafood. KDEs offer information to substantiate legality, species identification, sustainability, food safety, and food quality. Buyers and federal agencies may demand more data to document and ultimately establish the granularity of data that they seek from the traceability process. The efficient and effective exchange of this array of data relies on the existence of a common ontology or language. In information science, an ontology is formal naming and definition of the types, properties, and interrelationships between entities that enable discourse to occur (Bhatt and others 2016).

As reported in its "Seafood Traceability Proof of Concept Project Overview" (GS1 US 2014), GS1 US discovered how many combinations of formats that 5 participating companies used in data collection. Examples are shown in Fig. 6. GS1 US found variation in formats used for calendar date, KDEs for lot/batch/serial numbers, trading partners, item identifiers, and activity identifiers. A standardization scheme for data attributes is needed to enable more effective commercial data/information exchange.

KEY DATA ELEMENT	TRIDENT SEAFOOD	BUMBLE BEE FOODS	HIGH LINER FOODS	SEA PORT PRODUCTS	SLADE GORTON
CTE TYPE	Receive	Receive	Receive	Receive	Receive
CTE ID	TR001	BB001	HLF001	SP001	SG001
EVENT OWNER	0028029981070	0086600000015	0041600000007	0659878000003	0073129000008
DATE/TIME	8/25/2013 11:10-12:00	2011/07/07 0:0:00	1/7/2013	2013/05/14 6:25:00	9/23/2013
EVENT LOCATION	Warehouse	Preparation Facility	0041600000007	Cold Storage	Slade Gorton Warehouse
TRADING PARTNER	A Cannery	Distribution Center	837249	SPP8304	SG1398
ITEM ID (GTIN)	434937	100252	23007283	109457	85261
LOT/BATCH/SERIAL#	12QFF139	BBM11290	201212120097	4855	45003511080
QUANTITY	98	42831	1700	2077.16	8
UNIT OF MEASURE	Cases	Kilograms	Cases	Kilograms	Cases
ACTIVITY ID	928179	1122334455	12102726	C3100	4500235111
ACTIVITY TYPE	Purchase Order	Purchase Order	Purchase Order	Invoice	Purchase Order

Figure 6 – Proof of concept data spreadsheet. Adapted from GS1 US (2014). Reprinted with permission, GS1 US.

6.2 Flexibility, Customization, and Adaptability

Traceability interoperability standards need to be flexible enough to capture, store, and share custom CTEs and KDEs as the needs arise. Further, it is important that the mechanism for extensibility is accessible to all users, enabling them to customize and adapt a system's capabilities to suit their specific requirements. This is difficult to incorporate into the design given the challenges mentioned above, the need to accommodate more sophisticated and ambitious traceability systems as business relationships evolve, and implementation in regions with limited infrastructure and technological capabilities. Further, traceability may be used to support purposes beyond product movement and regulatory compliance. For example, KDE and CTE applications often need to represent additional events to present a complete product pedigree. Components of an organization's HACCP program relating to sourcing and distribution of perishable seafood may require temperature monitoring and pathogen testing, in addition to geo-location-based chain of custody. This could be accomplished by either creating additional CTE types for testing and temperature monitoring or adding KDEs linked to the standard CTEs.

Incorporating agreed "traceability best practices" for the various players in the seafood industry assists in minimizing the complexities that come with enabling flexible and adaptable systems. Best practices become the "traceability model" that forms the foundation upon which the above elements are put into practice. The overall context in which to place the foundation and main elements relates to the business objective(s) to be accomplished. The business objective(s), such as the examples shown in Fig. 3, determine the traceability model deployed, including the CTEs, and the depth, breadth, and precision of the KDEs recorded at each CTE.

Manage Risk	Create Business Opportunity
Recalls, withdrawals	Market access
Regulatory compliance	Supply chain efficiency
Chain of custody	Waste, cost reduction
Customer demands	Building consumer, buyer trust
Product quality	Product differentiation

Figure 7 – Examples of business objectives using traceability.

Other examples of extended traceability applications include consumer-facing applications, aquaculture-related processes, and sustainability metrics. Guidance for businesses and other stakeholders on the creation, sharing, and interpretation of custom CTEs and KDEs to ensure standards and traceability capabilities evolve with changing industry needs will be valuable. Traceability interoperability standards, therefore, need to be flexible enough to capture, store, and share custom CTEs and KDEs as the needs arise. Further, it is important that the mechanism for extensibility is accessible to all users.

6.3 Other Considerations

Other issues that require consideration in enabling the identification of products and processes, to achieve the effective and efficient exchange of data required for interoperable traceability include the following:

- What are the needs/requirements for each stakeholder group and their role?
- What are the functions of the groups?

- How will different systems be accessed and functionality be granted based on each role?
- Beyond essential compliance requirements, how will data access and system functionality decisions be governed with individual stakeholders?

Functional considerations for enabling the proposed technology architecture to produce interoperable traceability capabilities that are robust, resilient, and scalable are discussed in Sections 7 – 12.

There are also considerations surrounding the maintenance of a global traceability interoperability standard. Considerations that a standard-setting organization (such as GS1 and/or ISO [International Organization for Standardization]) would address would likely include:

- In which languages, other than English, does the standard need to be kept?
- What is the process for recommending and approving change to the standard(s)?
- How will governance of standards of acceptance be structured and function?

These types of considerations may occur at times in response to recommendations on support required to enable effective interoperability in the seafood industry (as made, for example, in the produce industry by the Produce Traceability Initiative's Leadership Council (PTI – LC)). They may also occur in the travel industry (by the OpenTravel Alliance Board of Directors (OTA–BD), for example) and in the finance industry (by the Registration Management Group (RMG), for example).

Another matter is measurement of goals, performance, and key objectives for: rollout, implementation and adoption, communications with stakeholders, milestones or stages, on-going maintenance (that is, value, cost, and percent adoption), data quality, and privacy and security. These and other considerations relate to return on investment to commercial businesses and industry usage factors that will reduce users' cost of operation and increase the system's contribution to public good.

The final consideration is socialization. How will industry stakeholders be motivated to commit to adhering to the protocols, processes, language, and technology solutions necessary for ensuring that the proposed architecture is successfully translated into practice? As faced by many complex information technology (IT) efforts, the socialization of stakeholders will play an important role in ensuring that the interoperable solutions that flow from implementation of the architecture continually improve and evolve in line with industry's needs. Strategically engaging various communities of practice in implementing the platform will broaden the socialization process required to encourage seafood firms to participate in and commit to implementation of the architecture, assist the development of whole-of-supply-chain solutions, and encourage the sharing of data required to enable interoperable traceability.

7. Global Registries

A global registry is an authoritative reference directory that keeps track of connections, guarantees the uniqueness of data, ensures compliance with agreed upon standards/practices, and manages rules established for use and authorization of connections for data. Often compared to a "traffic cop," the function of a global registry, which enables the interoperability of a distributed network, is quite simple—verification and authentication of data. Two examples of a global registry function are the GS1 Global Data Synchronization Network (GDSN) for Product Master Data and Nextgate's Provider and Organization Register (POR) for the health industry.

Registries are essentially files of information that meet a common standard or format which guide data "traffic" in order to minimize data errors that could otherwise undermine the effective and efficient exchange of data. The design and operation of registries required to enable the interoperability technology architecture could potentially follow processes similar to those used to establish the Product Master Data and Provider and Organization Register, for example.

A registry could also be used as a global reference to contain globally-agreed reference information, such as seafood-specific information (species, catch areas, gear types) or standards-related information (data standards, data dictionaries). These can be true global databases under the managed responsibility of an appointed organization such as FAO (for example, for fishing vessel finder) or ISO (for Certification Register).

8. Query and Response Mechanisms

A query and response mechanism is a key component required to enable the interoperability of internal and external traceability systems. Query and response mechanisms comprise a standardized data exchange interface (sometimes called a "portal") to enable multiple, distinct traceability applications or systems to create and share visibility event data, both within and across enterprises, and either on-demand or as scheduled. This sharing is aimed at enabling users to gain a shared view of physical or digital objects within a relevant business context.

A query often starts with a traceable entity identifier, and not necessarily with a CTE. Also, the data being made available by the information owner may exclude sensitive internal (business) information. Aspects of functionality needs are described below.

- Authentication – The query interface should provide a means for authenticating the client system's identity which is then used for authorization. Clients and responding systems may be linked to 1 legal entity (single tenant) or more than 1 legal entity (multi-tenant). Therefore, it may be necessary to provide the identity of both the client and the specific tenant.
- Authorization – Based on the identity of the client, the query response mechanism may respond in the following ways:
    - Refuse the query request
    - Respond with less data than requested. Examples include:
        - Only events submitted by the requesting client
        - Only events including products or locations related to the requesting client
        - Subset of events in order to meet performance expectations, such as response times to validate a system's speed, stability, and scalability
    - Respond with aggregate or summary information rather than specific details.
- On-Demand Queries – Receive and process client requests immediately through 2-way, synchronous binding.
- Scheduled Queries – Client creates a standing query and specifies the frequency and timing of execution. The response mechanism provides, according to the client-specified schedule, the data requested through a callback interface.

- Query Structure – answering the basic questions What, When, Where and Why, with attributes that include:
    - Event types
    - Date/Time range
    - Business(s)
    - Location(s)
    - Product(s) and Lots or Serial Numbers
    - Ingredient Product(s), Lots, and Serial Numbers
    - Quantity ranges
- Technology – Various communication technologies may be used to enable Query/Response. Examples include:
    - Web APIs including SOAP and REST
    - AS2 using XML

9. Virtual Lock Boxes

Another key component of the architecture is the Virtual Lock Box layer which allows each system owner to exercise control over who can access the data, when it may be accessed, and for what purpose. A Virtual Lock Box may be regarded as a set of requirements (functional, technical, and standards) which a TPSP must incorporate in its service offering in order to be certified to offer interoperability in the global food industry.

Examples of functionality include:

- Information owner managing access rights
    - Specify organization(s), role(s), user(s)
    - Point to a list of registered "consumers" of the data
    - Access right at CTE and KDE level
- Information owner managing usage rights
    - Specify share with others, "for your eyes only" (for example, license), keep or destroy (set time limit, expiration date)
    - Usage right at CTE and KDE level
- Information owner managing information content (traceability model, links, minimum compliance, adaptable content suited to different business objectives)
    - Manual input
    - Integration feeds from internal system
    - Diagnostic, modeling, and so on, tools for user-managed set-up
- Information validation (adherence to standards, content check)
    - Tools for compliance checking of data input (syntax and contents) against agreed data registries, standards protocols.

Examples of technical specifications are:

- API/communication protocols for data integration with data owner internal systems
- API/communication protocols for adhering to specifications required by "discovery service" provider(s).

Examples of types of standards are:

- Traceability protocols (minimum agreed, flexible standards)
- ID schemes (syntax) for company, premise, traceable entities, CTEs, and KDEs.

10. Data Authenticity

In regards to data authenticity and data validation and verification, the capability is needed to distinguish between data that can be verified against "global directories" (compliance with standards, and product and place identifiers against global reference data registries) versus an individual company's KDEs. While missing KDEs can be flagged, erroneous data content (whether through errors or malicious intent) is more difficult to detect. While some errors may be caught through software checks, certification and audit schemes, which are outside the scope of this document, will play roles here.

10.1 Data Validation and Verification

The FDA has defined validation and verification (21 CFR Part 117.3) as follows:

Validation – "Obtaining and evaluating scientific and technical evidence that a control measure, combination of control measures, or the food safety plan as a whole, when properly implemented, is capable of effectively controlling the identified hazards." Validation plays an important role in establishing the KDEs required to enable interoperable traceability.

Verification – "The application of methods, procedures, tests and other evaluations, in addition to monitoring, to determine whether a control measure or combination of control measures is or has been operating as intended and to establish the validity of the food safety plan." Verification plays an important role in ensuring KDEs are correctly entered.

To ensure that the information at the end of the chain is meaningful, it is important that:

- Information that has been entered at the start of the traceability system is true and accurate, and
- Information has not been tampered with while passing through the supply chain.

To assure accuracy of the information at all stages in the chain, a level of data validation and verification should take place. Assurance is defined by the ISEAL Alliance (2016), the global membership association for sustainability standards, as: "Demonstrable evidence that specified requirements relating to a product, process, system, person, or body are fulfilled (adapted from ISO 17000)."

As a practical example, fish, especially filleted, are vulnerable to mislabeling and fraud without taxonomical verification or DNA speciation. The reported incidence of mislabeling in the international seafood industry, determined on the basis of DNA testing, varies from an average estimate of less than 1% for MSC-labeled seafood (MSC 2016) to as high as 30% during the past 5 years (Pardo and others 2016) for uncertified products. The occurrence of mislabeling shows both the challenge around data validation and verification and the importance of improving traceability through effective interoperability. Mislabeling can be either accidental or intentional. Accidental mislabeling can be addressed through improved training and internal processes, technical data validation solutions, and internal audits. Intentional mislabeling will require third-party auditing of government, downstream supply chain partners, and/or independent certification schemes.

At this time, DNA testing has limitations as a method of verification. DNA testing can be costly to conduct on a large scale, and is generally limited to distinguishing between species, which is useful although potentially challenging. For example, in the case of canned tuna, defining species using DNA primers can be difficult as a result of the high heat of commercial sterilization processing of tuna meat.

Verification of harvest location by trace element fingerprinting remains the ultimate goal of chemists, although species identification is helpful in this regard. In general, the country of origin of farmed shrimp is difficult to determine by DNA or trace-element fingerprinting because ponds often have liners that block soil, sediments, standardized filtered water, and feeds that would otherwise give distinguishing geographical characteristics to the shrimp.

Until DNA verification methods have been successfully developed, tested, and expanded to all commercial species of seafood, the main method of verification will remain auditing of facilities and records.

Some initiatives are taking place to automate verification of records. An example is the proposed EU Illegal, Unreported, and Unregulated (IUU) Regulation to combat illegal fishing practices (EJF and others 2016). The regulation proposes control of IUU fishing through: (1) catch certification scheme, (2) penalties proportional to the economic value of the catch, and (3) regular publication of IUU vessels as identified by the RFMOs (Regional Fisheries Management Organizations). Currently, the EU Commission is establishing a database of some 250,000 catch certificates received each year. Such an electronic catch certificate database can ensure that catch certificates are not used multiple times, exceeding the total volume of the certificate. However, France, Germany, Italy, The Netherlands, Spain, and the United Kingdom are the 6 largest importing nations of fishery products outside the EU, in which 73% of the total volume may be subject to IUU. Thus, the EU catch certificate program has its limitations.

In the United States, NOAA is charged with combatting IUU fishing. In a report to Congress in 2013, the National Marine Fisheries Service (NMFS), an office of NOAA, identified 10 nations having IUU fishing concerns (NOAA 2015). In April 2015, the National Ocean Council Committee on Illegal, Unreported and Unregulated Fishing and Seafood Fraud was established. The committee, comprised of 14 federal agency-members, takes the place of the Presidential Task Force on Combating IUU Fishing and Seafood Fraud and oversees implementation of the Task Force Action Plan released in March, 2015 (IUU Fishing and Seafood Fraud Web Portal 2016). NOAA has developed its own IUU program on “at risk” species which will require entry of specified KDEs into the government database—the International Trade Data System (ITDS). The program will likely be finalized by the end of 2016.

10.2 Data Governance

In this area, there is the need to distinguish between governance of global industry standards and reference data versus those for company-specific data. Additional factors are:

- Anchoring governance of the technology architecture for interoperable food traceability with a not-for-profit global body (following examples such as ISO, GS1, and Forest Stewardship Council) to provide the necessary oversight and direction.
- Specific reference data and ontologies (such as seafood species, catch areas, and gear types) should be delegated to a relevant body (such as FAO) for global responsibility for information maintenance and provision of access.

- Global standards governance should also rest with a global body, such as ISO, while industry-led organizations (such as GS1) could provide standards (such as IDs) and related services to industry players.
- Company-specific data are governed by general technology standards and relevant regulations and schemes for each information owner.

11. Syntactic and Semantic Interoperability: Ontology and Taxonomy

Enabling interoperability between previously heterogeneous software requires that these systems have the ability to communicate effectively by sharing standardized unambiguous packages of data. The foundational prerequisite of this is 2 or more information technology systems having the ability to communicate on a transactional level through the sharing of a standardized process for packaging and exchanging data. This ability is called **syntactic interoperability**. The development of a common language (ontology) enables 2 or more systems to not only exchange data at a transactional level but to converse in ways that result in a shared sense of meaning, thus providing the potential for the creation of new knowledge. This ability is **semantic interoperability**.

While these 2 levels of interoperability overlap, it is important to differentiate between them. The reasons for this include that the determinants of the ability and motivation of businesses to implement effective interoperable traceability systems, such as access and usage rights, differ for syntactic and semantic interoperability. For example, unless a strong collaborative and trusting relationship exists between businesses, it is unlikely that they are prepared to exchange the potentially sensitive data and invest the resources required to utilize semantic interoperability for the purposes of acquiring competitive advantage. A useful analogy is absorptive capacity where businesses have the ability to recognize, assimilate, and use knowledge for commercial advantage through complementary resources and the ability to interact and subsequently innovate in increasingly sophisticated ways (Lane and Lubatkin 1998).

Achieving syntactic interoperability rests on systems communicating the “what” and “how” data that relate to internal and external traceability. Internal traceability is that which occurs within a business. External traceability is that which occurs outside of a business’ operations. Common standardized CTEs and KDEs are critical to enabling internal and external systems to interact effectively and efficiently. So too, is the existence of appropriate processes within the participating businesses (for example, unique and linked product identifiers, common batch sizes) and the existence of complementary external enablers (for example, technology infrastructure, trained users) between the participating businesses. This ensures that the exchanged data are accurate, verifiable, and capable of being used appropriately for commercial or governance-related purposes.

Achieving semantic interoperability rests on the existence of a common language (which encompasses ontology and taxonomy protocols/standards) to which internal and external traceability systems adhere. This enables greater supply chain transparency. Achieving a common language rests on the existence of common standardized terminology and a hierarchy of terms or identifiers. In seafood, this ontology is arguably the greatest challenge facing the establishment of interoperable traceability. The extent to which a common ontology does not exist is illustrated by differences between nationally identified species. The Canadian Food Inspection Agency (CFIA) lists nearly 800 species of seafood; the U.S. Food and Drug Administration (U.S. FDA) lists more than 1,800 species. Similarities between the CFIA and FDA lists total approximately 500 species.

When one expands this parallel to differences in species listed by countries worldwide, and differences in terminology used to identify catch location, the need to establish a common ontology quickly becomes evident, particularly as misalignments in terminologies create significant compliance challenges and limit the effectiveness of traceability efforts. A possible solution to some species-related challenges is the use of common Global Trade Item Numbers (GTIN). Electronic Product Code Information Services (EPCIS) and Electronic Data Interchange (EDI) are examples of communication standards that could be used in the development of systems that enable semantic interoperability. It is important to note that semantic interoperability does not necessarily mean a universal language, it instead can be a set of semantic relationships that enable common meanings to be determined when moving data across domains.

12. Draft Technical Specifications

The document concludes by discussing specific components required to implement effective and efficient interoperable seafood traceability by achieving the outcomes and performance capabilities described in previous sections. Potential solution providers and next steps are also discussed.

12.1 Technical Challenges and Considerations

Bhatt and others (2016) described the complexities of achieving fully interoperable information technology in seafood. The seafood industry operates in a far wider variety of environments and locations than most industries that have established interoperable technology solutions, handles many hundreds of species, and manufacturers an enormous array of processed products. Therefore, the intended interoperable traceability platform needs to achieve something that has not been previously achieved in food and agriculture, nor in other industries to the same level of complexity.

Other considerations that need to be factored into the choice of technical solutions include, for example:

- The fresh produce industry primarily uses printed labels to enable operability to occur between businesses situated along the supply chain, and it has a narrower range of products.
- The produce industry has fewer products that can be substituted for one another, either by accident or fraudulently.
- The seafood industry does not have the financial resources and does not operate in the strong regulatory environment that played an important role in enabling interoperability in the financial industry.

Five years ago it would have been extremely difficult, potentially even unfeasible, to have overcome this series of inherent challenges (Krueger 2016). Rapidly evolving technologies are used in other fields and can be woven together into a series of components that together form an integrated solution. The process of integration will be complicated; one of the first considerations is to decide how to manage the process.

This oversight role is separate from the governance approach described earlier for data management, establishment of technical standards and protocols, and language/communication. This is not about how the requirements are established and maintained, but how technical requirements are translated into specifications for development and implementation of the technology architecture. Ensuring that specifications and capabilities evolve in line with industry's needs is critical to the sustainability of any system. Important early decisions include determining who will lead the translation of technical requirements into detailed specifications and selecting and then contracting the required TPSPs.

The process of selecting and then contracting the required TPSPs may itself require knowledge and skills that must be acquired through training or other means. Considerations must also be given to the committed stakeholders that need to participate in this process. For example, from what regions of the world should they emanate; what experiences must they have to play an active, valuable role in determining specific technology requirements/specifications; and what mix of proactive champions versus businesses that are highly sensitive about data sharing should the partnership group comprise? Choosing how and who to manage the development process is an important early decision.

Open source solutions are promoted by a number of interoperability initiatives, including, for example OpenTravel Alliance (2016). An important potential benefit of following an open-source approach is how it enables platform participants, along with technology providers or firms, to contribute capabilities or improvements to the platform. This gets to the licensing strategy with the options ranging from open source for review only, to open source that allows participant contributions to be applied to the platform core, or open source that allows derivative works and installation elsewhere. As shown by technology solutions such as WSO2, for example, which is based on open-source tools with a proprietary integration layer, the platform does not have to be fully open source to gain the benefits of open source. How far to proceed in terms of pursuing development of open-sourced solutions needs to be determined at the outset.

12.2 Strategy

In addition to reasons described above, the purpose of the interoperable technology infrastructure, and the degree to which it could be extended to other functionalities also requires a different approach to the architecture's design and specifications than those which has been used in interoperability solutions established in other industries and sectors (for example finance, travel, automotive, and produce).

No single solution provider has the end-to-end expertise required to provide all of the components necessary to implement the proposed technology architecture. A partnership of technology providers and communities of practice are required to advance both the core platform and improve the value produced by each element of its design. The technology platform will essentially serve as middleware to the many specialized and diverse data systems already in use by seafood firms, with each core technical function provided by a different technology partner.

Using open-source solutions would increase stakeholder acceptance, by making software free to anyone who wishes to participate, and ensuring transparency on the overall approach while simultaneously ensuring users abide by technical roadmaps and established governance processes (Perini 2007). Open source options also benefit from the ability to leverage stakeholder enhancements (Hicks and Pachamanova 2007) and lead to increased transparency that in turn results in increased security, as identified by the Department of Defense (DOD 2009) in a guidance document relating to open-sourced software. The technical solution should have sufficient use case-based scalability so that stakeholders have the functionality required for them to find value for using the architecture based on their current state of preparedness for implementing interoperable traceability. This includes enabling organizations to build custom extensions for special use cases.

The use of open standards is both easier to achieve and more effective through the use of a semantic ontology capability, and engaging communities of practice (Bates 2014). Wenger-Trayner and Wenger-Trayner (2015) describes communities of practice as “groups of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly.” An example of the benefits from use of open-sourced options and communities of practice in the development of interoperability solutions is that while there are industry accepted species names, a firm’s internal systems can use other names without compromising interoperability.

12.3 Example Solution

The strawmodel technology architecture shown in Fig. 2 reflects a functioning architecture. The following section presents a brief description of components that could potentially provide an effective and efficient solution to enabling interoperable seafood traceability.

The 4 core technology components of a viable system are: Host, Security, Automated Query & Response Portal, and Global Registries. Figure 8 illustrates how the 4 technology components of this particular architectural solution are arranged and interact to form a viable system. The purpose of each component, and potential service providers are then addressed.

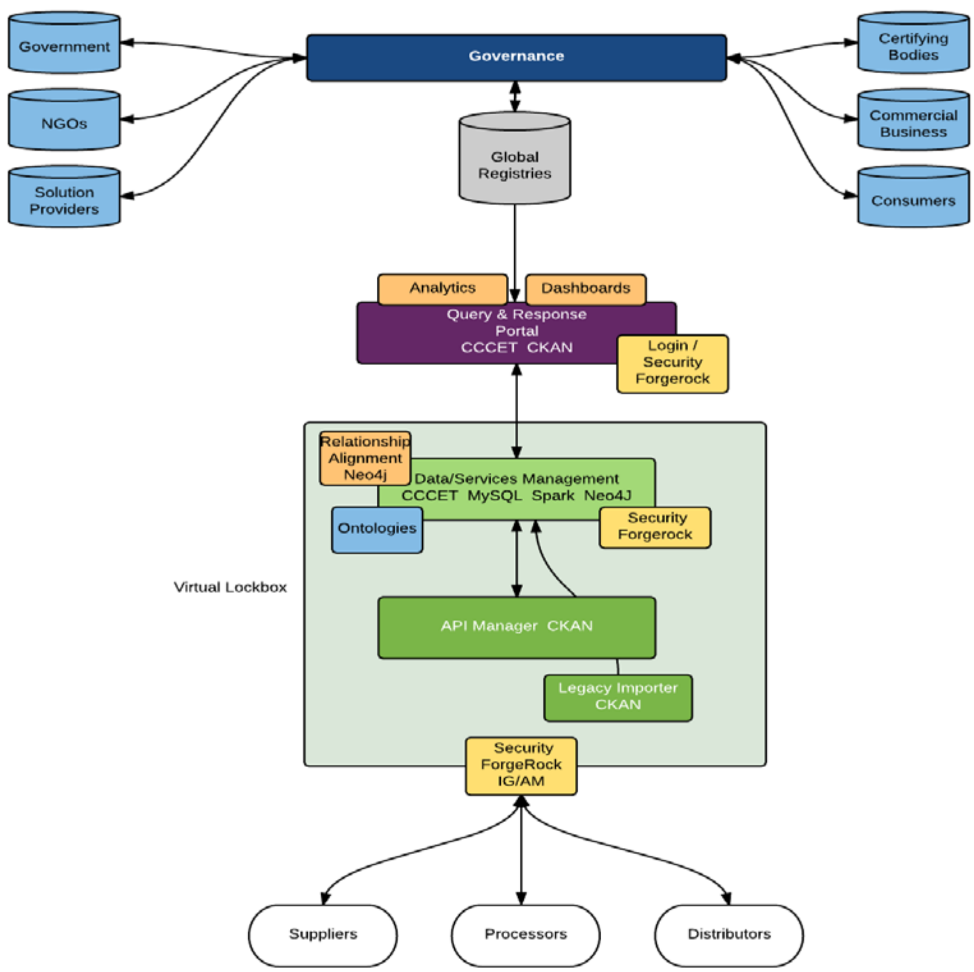

Figure 8 – Potential solution to the proposed technology architecture to enable interoperability.

Host

How interoperability solutions are hosted and where data are stored are important considerations from security, access, commercial sensitivity, and legal perspectives. One option is to enable the various architectural components to seamlessly interact through hosting them via a cloud service provider. The physical location of the host is a governance decision.

Given the global nature of the seafood industry, the data privacy laws of multiple countries must be considered. One of the concepts important to the architecture's design is ensuring the retention of data by individual businesses. This is important for meeting data sovereignty requirements imposed by jurisdictions, including the EU and Australia, which require data to be housed locally.

Security

The need for security is identified in the Structural Principles. In practice this breaks down into cloud/server security, access and identity security, and compliance.

Cloud/server security provides host-based security protection, such as anti-malware, firewalls, intrusion prevention and detection, log management, and file integrity.

Access and identity security ensures that only approved users enter the system, and that their access to specific data and information is controlled. Dealing with the different standards used across technology firms becomes a challenge. Some solutions use adaptive intelligence to continuously protect against risk-based threats while allowing end users fine-grained access to their data.

Compliance systems continuously monitor and audit the system infrastructure to provide visibility and operational awareness of what is occurring in it. This includes identification of any anomalies that may need to be addressed.

Automated Query & Response Portals

These components translate into data management tools and APIs, providing a streamlined path to make data discoverable and presentable with dataset-specific pages and metadata as the foundation (Willmes and others 2014). Available solutions also enable data entry via web interfaces and custom spreadsheet import tools, which are designed to allow harvesting of data from existing organization repositories to minimize requirements for keyword searches, tags, and browsing capabilities.

Global Registries

Because they have their own validation and certification protocols, global registries can simplify the amount of data that is subject to certification. The registry hub houses the primary registration data needed to identify the "who, what, when and where" for premises, products, participants, actions, and related fields. This platform can be purpose-built or existing platforms could be used to develop systems that have the capabilities required to bring together the multiple technologies detailed above. The function of the global registry is based on how much standardization is anticipated and required. At its core, the capability of global registries is driven by a central registry hub that has relationship mapping capabilities and big-data management tools.

Relationship mapping can be accomplished via graphical displays of data, which have become increasingly popular for identifying connections because the topology of the data (such as what the supply chain looks like) can be more useful than the data itself (Reutter and others 2016). Relationship mapping is often used to focus on single element, product, entity, or other element, and show the connections of that to other items in the database. This would enable, for example, a processor to find out which of their products uses an ingredient from the same upstream source.

As registry hubs encounter multiple layers of different types of data from a diverse set of inputs, it is generally preferable to use big data processing engines.

12.4 Potential service providers

Described below are examples of potential service providers for each of the four components.[4] The list of service providers and solutions discussed is non-exhaustive.

Hosts

Amazon Web Services (AWS) is an example of a leading provider that can provide high-level security for private sector users. AWS is also the largest web service provider, with the biggest community of developers and companies of any platform for continued platform advancement (Asay 2015). There are more than 500 peer-reviewed journal articles mentioning AWS tools as part of their subject or in the methods used for data collecting/sharing.

Security

With all web services, security relies on a shortlist of factors. These factors include establishing a security strategy before deciding on tools and controls, addressing compliance needs and regulations from the outset, and establishing users' responsibilities and liabilities (Moore 2016). There are currently 19 AWS-approved vendors for cloud/server security protection, including anti-malware, firewalls, intrusion prevention and detection, log management, and file integrity. Trend Micro's Deep Security Suite is one of the most broadly accepted market leaders, and the only one of those 19 in the AWS Quick Start (2014) list for gold-standard deployments.

Access and identity security providers include ForgeRock, a solution that uses a Security Token Service to overcome the challenge of standards differing between technology firms. ForgeRock is the only open-source identity and commercial access management platform on the market (ForgeRock 2016). ForgeRock won the Cyber Defense Magazine's "Best Product in Identity and Access Management" award (Cyber Defense Magazine 2015).

Compliance service providers include Evident.IO, an example of a solution developed specifically to fit the AWS shared-responsibility model. Another example is CloudCheckr, which provides compliance to HIPAA (Health Insurance Portability and Accountability Act), PCI DSS (Payment Card Industry Data

---

[4] Disclaimer: The IFT GFTC does not recommend or critique specific technology solution providers but instead has chosen to list a few examples of technologies to highlight the kinds of functionalities needed. Further, we emphasize the fact it is not envisioned that the wheel be reinvented per se, but instead an attempt be made to stitch together existing technologies for the purpose of enabling interoperability of food traceability.

Security Standard), FSMA (Food Safety Modernization Act), and other major compliance requirements, and also assists in compliance with EU/Australian data regulations. Two other examples of vendors providing data security services include Sumologic and Splunk, which extend security of machine data and logging, and provide more advanced operational intelligence.

Automated Query & Response Portals

Examples of data management tool providers include CKAN, whose solutions enable data entry via web interfaces, JSON APIs, and custom spreadsheet import tools.

Global Registries

An example of a relationship mapping solution is Neo4j, which has the largest development community, Neo4j is applied in a number of highly complex fields, such as biological networks, and has been used to manage databases that are too complex for desktop computers (Summer and others 2015).

Examples of big data solutions include tools developed by AWS to leverage a broad array of specialized applications. Apache Spark is a fast and generally open-source engine that has rapidly expanded into fields as diverse as neuroscience (Boubella and others 2016) and smart grid technologies (Shyam and others 2015). Snowflake Elastic Data Warehouse is not open source, but has the advantage of being designed to handle semi-structured data (Snowflake 2015). While not open source, Zoomdata simplifies the ability to view data from multiple sources appearing as from a single source (Gutierrez 2016). Each of these has data analytics capabilities, and the CCCET Framework SCOREcard is an example of an open-source application developed for the FDA for summarization and display of real-time data analytics (Krueger 2016).

Potential registry hub solutions include WSO2 and the Global CCCET framework. WS02 uses open-source tools with a proprietary integration layer, is componentized for scalable deployment, and uses a central data storage model (Siriwardena 2016). The Global CCCET framework uses open-source software with middleware tailored for existing food and agriculture applications (Krueger 2016). The ability to connect previously heterogeneous components together enables the overall interoperability solution to evolve as users' system capacity or functionality needs change.

V. Future Directions and Next Steps

This specifications and design document is an interim research output that will evolve through further vetting and peer review, resulting in a technology architecture that is resilient and robust, and which meets industry's needs. Activities to engage industry stakeholders in the continued development and implementation of a technology architecture for enabling interoperable traceability include the ongoing creation of awareness, education, and training tools, and:

- Review by subject matter experts in traceability, food industry, and information and communication technology
- Peer-review by a select group of experts including but not limited to:
  - "Global Dialogue" process being led by the World Wildlife Fund and the IFT GFTC

    - Future of Fish disruptive business ecosystem and technology pods[5]
    - FishWise traceability team and associated resources[6]
    - Harmonization with the catch documentation and traceability system that is being developed by the USAID Oceans Partnership for the ASEAN region[7]
    - Alignment with the Consumer Goods Forum Interoperability Initiative
- Creating awareness of the blueprint and seeking feedback through presentations at conferences and scientific meetings
- Educating through a series of webcasts and/or in-person consultations with relevant stakeholders
- Implementing training through the development of resources that include a roll-out strategy guide
- Development of case studies to demonstrate the application of the architecture for individual supply chain stakeholders
- Increasing the granularity of the technology architecture based on additional research and development work conducted by technology experts
- Creating public-facing content on the web and in print for distribution to relevant stakeholders
- Setting the stage for piloting the proof of concept and measuring the impact of enabling this interoperable architecture in a controlled study within the industry.

VI. Acknowledgements

The GFTC greatly appreciates the deliberations and input to this effort and document that was provided by the members of the Technology Architecture Working Group. Contributors included Barbara Blakistone, Vice President of Aquatic Food Products at IEH Laboratories; Steven Mavity, Senior Vice President of Technical Services and Corporate Quality at Bumble Bee Foods; Titia Sjenitzer, Senior Product Integrity Manager at the Marine Stewardship Council; Brian Sterling, President and CEO of SCS Consulting; Michele Southall, Industry Engagement Director, GS1 US; Andy Kennedy, President, Foodlogiq; Helge Kittilsen, Region Manager, North America, Trace Tracker Canada; Rosetta Newsome, Director of Science and Policy Initiatives, Institute of Food Technologists; GLOBAL CCCET (Eric Hoffman, Shaun Kennedy, Bill Krueger); and Gil Sylvia, Director, Coastal Oregon Marine Experiment Station, Oregon State University.

[5] http://www.futureoffish.org/pods
[6] https://www.fishwise.org/traceability/traceability-resources/
[7] https://www.usaid.gov/asia-regional/fact-sheets/oceans-and-fisheries-partnership

VII. Abbreviations and Glossary

API – Application Programming Interface. A set of rules and specifications for software programs to follow in communicating with each other to facilitate/enable interoperability (Proffitt 2013; Stackflow.com 2011).

AS2 – Application Statement 2. A specification that enables the secure exchange of data through a secure connection (Moberg and Drummond 2005).

Code – A set of rules and specifications for software programs to follow in communicating with each other to facilitate/enable interoperability (Stackflow.com 2011).

CTE – Critical Tracking Event. A point at which product is moved between premises or is transformed, or which is determined to be a point at which data capture is necessary to maintain traceability (Bhatt and others 2016).

EDI – Electronic Data Interchange

EPCIS – Electronic Product Code Information Services

Extensibility – Ensuring the ability to extend a system's functions/capabilities during its design (Rodriguez and Cibraro 2009)

FSMA – Food Safety Modernization Act 2011, which established standards for the gathering, reporting and storage of data and information pertaining to production, processing, and distribution of domestic and imported products in the U.S. food industry (FDA, 2017).

GDSN – Global Data Synchronization Network. An internet-based interconnected network of interoperable data pools and a global registry known as the GS1 Global Registry, that enables companies around the world to exchange standardized and synchronized supply chain data with their trading partners using a standardized Global Product Classification (GS1 2016)

GTIN – Global Trade Item Number. The format in which GTINs must be represented in the 14-digit reference field (key) in computer files to ensure uniqueness of the identification numbers (Bhatt and others 2016).

HIPAA - Health Insurance Portability and Accountability Act 1996, which established privacy safeguards to prevent unauthorized access to data pertaining to individuals' medical records and associated information including benefit plans (ASPE, 1996).

KDE – Key Data Element. Input required to successfully trace a product and/or its ingredients through all relevant CTEs (Bhatt and others 2016).

Ontology – In information science, a formal naming and definition of the types, properties, and interrelationships between entities that enable a particular type of discourse to occur (Bhatt and others 2016).

PCI DSS – Payment Card Industry Data Security Standards, overseen by the global forum PCI Security Standards Council, which guide the development, enhancement, storage, dissemination and implementation of security of data pertaining to financial accounts and transactions.

REST – Representational State Transfer. The software architecture style that is utilized by the World Wide Web within a hypermedia system (Fielding 2000).

Semantic interoperability – The ability of information systems to not only exchange unambiguous data that 2 or more systems understand, but also enable computerized systems to converse in ways that result in a shared sense of meaning and the creation of new knowledge (Bhatt and others 2016).

SOAP – Simple Object Access Protocol. A protocol used for structuring data communications between the World Wide Web and computer systems (Skonnard 2003).

Syntactic interoperability – The ability of 2 or more information technology systems to communicate through a standardized process for packaging and sharing data, the prerequisite for functional interoperability (Bhatt and others 2016)

XML – eXtensible Markup Language. A schemas technology which is a W3Consortium standard.

VIII. References

Asay M. 2015. AWS now 10X the size of its competitors: is the cloud arms race over? TechRepublic May 20. CBS Interactive. Available from: http://www.techrepublic.com/article/aws-now-10x-the-size-of-its-competitors-is-the-cloud-arms-race-over/. Accessed 2016 November 16.

ASPE. 1996. Health Insurance Portability and Accountability Act of 1996. Office of The Assistant Secretary for Planning and Evaluation. Washington D.C. Available from: https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996

AWS Quick Start. 2014. AWS Quick Starts. Available from: https://aws.amazon.com/quickstart/. Accessed 2016 August 24.

Bates T. 2014. The role of communities of practice in a digital age. Online learning and distance education resources. October 1. Available from: http://www.tonybates.ca/2014/10/01/THE-ROLE-OF-COMMUNITIES-OF-PRACTICE-IN-A-DIGITAL-AGE/. Accessed 2016 November 5.

Bhatt T, Cusack C, Dent B, Gooch M, Jones D, Newsome R, Stitzinger J, Sylvia G, Zhang J. 2016. Project to develop an interoperable seafood traceability technology architecture: issues brief. Comp Rev Food Sci Food Saf 15(2):392–429.

Boubela RN, Kalcher K, Huf W, Našel C, Moser E. 2016. Big data approaches for the analysis of large-scale fMRI data using Apache Spark and GPU processing: a demonstration on resting-state fMRI data from the human connectome project. Front Neurosci 9:492-500. doi:10.3389/fnins.2015.00492.

Bours H, Han J, Hanaoka W, King S, Knowles O, Partridge E, Thomas K, Tolvanen S, Trenor T. 2013. Out of line: the failure of the global tuna longline fisheries. Dawe A, Leal I, Partridge E, editors. Amsterdam, The Netherlands: Greenpeace International. 44 p. Available from: http://www.greenpeace.org/international/Global/international/publications/oceans/2013/459-OutOfLineReport-DEF-LR.pdf. Accessed 2016 November 16.

Cyber Defense Magazine. 2015. CDM INFOSEC Award Winners 2016. Available from: http://www.cyberdefensemagazine.com/2016-cdm-infosec-award-winners/. Accessed 2016 August 24.

DOD. 2009. Clarifying guidance regarding open source software (OSS). Memorandum. October 16. Chief Information Officer. Department of Defense. Available from: http://dodcio.defense.gov/Portals/0/Documents/OSSFAQ/2009OSS.pdf. Accessed 2016 August 25.

EJF, Oceana, The Pew Charitable Trusts, WWF. 2016. The EU IUU regulation: building on success, EU progress in the global fight against illegal fishing. Environmental Justice Foundation, Oceana, The Pew Charitable Trusts, and World Wildlife Fund. Available from: http://www.iuuwatch.eu/wp-content/uploads/2015/07/IUU_report_010216_web.pdf. Accessed 2016 November 16.

FDA. 2017. FDA Food Safety Modernization Act (FSMA). U.S. Food & Drug Administration. U.S. Department of Health and Human Resources. Silver Spring, MD. Available from: https://www.fda.gov/Food/GuidanceRegulation/FSMA/

FFEIC. 2012. Supervision of technology service providers. IT examination handbook. Federal Financial Institutions Examination Council. Available from: http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_SupervisionofTechnologyServiceProviders(TSP).pdf. Accessed 2016 November 16.

Fielding RT. 2000. Chapter 5: Representational state transfer – REST. Donald Bren School of Information and Computer Sciences. University of California, Irvine. Available from: https://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm.

ForgeRock. 2016. Identity for everyone and everything. ForgeRock. Available from: https://www.forgerock.com/.

GS1 US. 2014. Seafood traceability proof of concept project overview. GS1 US Seafood Traceability Readiness Program. R1.1. Nov. 19. Available from: file:///C:/Users/rlnewsome/Downloads/GS1US_Seafood_Proof_of_Concept_Report_LR.pdf.

GS1. 2016. Global data synchronisation network (GDSN). May 2016. Lawrenceville, N.J. Available from: http://www.gs1.org/gdsn. Accessed 2016 November 16.

Gupta S. 2008. Definition, meaning and characteristics of principles of management. Available from: http://www.publishyourarticles.net/knowledge-hub/business-studies/principles-of-management/980/. Accessed 2016 November 16.

Gutierrez D. 2016. Zoomdata simplifies the development of data-driven applications with advanced visual analytics. April 24. Portland, Ore.: Inside Big Data. Available from: http://insidebigdata.com/2016/04/24/zoomdata-simplifies-the-development-of-data-driven-applications-with-advanced-visual-analytics-2/. Accessed 2016 November 16.

Hicks C, Pachamanova D. 2007. Back-propagation of user innovations: the open source compatibility edge. Bus Horizons 50(4):315–24.

ISEAL Alliance. 2016. Available from: www.isealalliance.org. Accessed 2016 April 12.

IUU Fishing and Seafood Fraud Web Portal. 2016. National Ocean Council Committee on IUU Fishing and Seafood Fraud. Available from: http://www.iuufishing.noaa.gov/Home.aspx. Accessed 2016 April 12.

Kittelsen H. 2016. Feedback/input from Helge Kittelsen on the Interoperable Traceability Technology Architecture (ITTA). March 21. Personal communication.

Krueger W. 2016. Global CCCET SCOREcard. Minneapolis, Minn.: Global CCCET. Available from: http://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiohZzNrsLPAhVGXB4KHZ0gAOoQFggeMAA&url=http%3A%2F%2Fdenver.afdo.org%2Fuploads%2F1%2F5%2F9%2F4%2F15948626%2F800-fpd-krueger.pptx&usg=AFQjCNEcT8UgUhtP6OaKgbBxLaWxoRF9Mg. Accessed 2016 November 16.

Lane PJ, Lubatkin M. 1998. Relative absorptive capacity and interorganizational learning. Strategic Manage J 19:461–77.

Mavity S, Blakistone B, Portochar M. 2012. Product traceability in the seafood supply chain. Webinar. McLean, Va.: National Fisheries Institute. Available from: http://www.gs1us.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=735&PortalId=0&TabId=785. Accessed 2016 November 22.Moberg D, Drummond R. 2005. AS2 for business data interchange using HTTP. July. Available from: https://www.ietf.org/rfc/rfc4130.txt.

Moore L. 2016. The top 7 AWS security issues: what you need to know. Threat Stock Blog and Cloud Security News. Threat Stock. Available from: http://blog.threatstack.com/what-you-need-to-know-about-the-top-7-aws-security-issues. Accessed 2016 November 28.

MSC. 2016. From ocean to plate: how DNA testing helps to ensure traceable, sustainable seafood, L. Anderson. Marine Stewardship Council. Available from: https://www.msc.org/documents/chain-of-custody-documents/from-ocean-to-plate.

NFI. 2015a. Comments submitted July 31, 2015 to the Presidential Task Force on Combatting Illegal, Unreported, and Unregulated Fishing and Seafood Fraud Action Plan Recommendations 14/15; determining types of information and operational standards related to data collection. Docket No. NOAA-NMFS-2014-0090-0265. McLean, Va.: National Fisheries Institute. Available from: http://www.regulations.gov/#!docketBrowser;rpp=25;po=0;s=national%252Bfisheries%252Binstitute;D=NOAA-NMFS-2014-0090.

NFI. 2015b. NFI top ten list. Nov. 2. McLean, Va.: National Fisheries Institute. Available from: http://www.aboutseafood.com/?s=list+of+top+ten.

NFI and GS1 US. 2011. Traceability for seafood: U.S. implementation guide. March. Version 1.1. National Fisheries Institute in association with GS1 US. Available from: http://www.aboutseafood.com/sites/all/files/FINAL%20Seafood%20Trace%20Guide_v1.1.pdf.

NOAA. 2015. Improving international fisheries management. Report to Congress pursuant to section 403(1) of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006. February. U.S. NOAA Fisheries. National Oceanic and Atmospheric Administration. Washington, D.C.: Dept. of Commerce. Available from: http://www.fisheries.noaa.gov/ia/iuu/msra_page/2015noaareptcongress.pdf. Accessed 2016 April 28.

NOAA. 2016. Magnuson-Stevens Fishery Conservation and Management Act. Seafood import monitoring program: proposed rule. U.S. NOAA Fisheries. National Oceanic and Atmospheric Administration. Washington, D.C.: Dept. of Commerce. Available from: https://www.federalregister.gov/documents/2016/02/05/2016-02216/magnuson-stevens-fishery-conservation-and-management-act-seafood-import-monitoring-program.

OpenTravel Alliance. 2016. Introduction to OpenTravel 2.0: overview, benefits and development process. Available from: http://opentravel.org/Resources/Uploads/PDF/OpenTravel2Intro.pdf. Accessed 2016 October 6.

Pardo MÁ, Jiménez E, Pérez-Villareal B. 2016. Misdescription incidents in seafood sector. Food Control 62:277-83.

Perini V. 2007. Leveraging open standards for collaborative commerce. Available from: www.opentravel.org/resources/uploads/pdf/uic_2007.pdf.

Proffitt B. 2013. What API's are and why they're important. Readwrite. September 14. Available from: http://readwrite.com/2013/09/19/api-defined/. Accessed 2016 November 16.

Reed H. 2006. Principles of interoperability and integration. Volume 1: Fundamentals. McLean, Va.: MITRE Corporation. Available from: https://www.mitre.org/sites/default/files/pdf/06_1124.pdf. Accessed 2016 April 28.

Reutter JL, Romero M, Vardi MY. 2016. Regular queries on graph databases. Theory Comput Syst April. doi:10.1007/s00224-016-9676-2.

Rodriguez J, Cibraro P. 2009. WCF extensibility guidance – introduction. Tellago, Inc. October. Microsoft. Available from: https://msdn.microsoft.com/en-us/library/ee667276.aspx. Accessed 2016 November 16.

Ross DT, Goodenough JB, Irvine CA. 1975. Software engineering process principles and goals. SofTech, Inc. Computer 17-27. May. Available from: https://www.computer.org/csdl/mags/co/1975/05/01649428.pdf. Accessed 2016 April 28.

Siriwardena S. 2016. Thirty solution patterns with the WSO2 identity server. Facilelogin. April 24. Available from: https://medium.facilelogin.com/thirty-solution-patterns-with-the-wso2-identity-server-16f9fd0c0389#.y3pin8nlo. Accessed 2016 November 16.

Shyam R, Bharathi Ganesh HB, Sachin Kumar S, Prabaharan Poornachandran, Soman KP. 2015. Apache Spark a Big Data Analytics Platform for Smart Grid. SMART GRID Technologies, August 6-8, 2015. Procedia Technology 21:171-78. Science Direct. Available from: http://ac.els-cdn.com/S2212017315003138/1-s2.0-S2212017315003138-main.pdf?_tid=b4dfa20a-b279-11e6-b0b1-00000aab0f6b&acdnat=1480014827_cb9937c813cb144f9efc306645a2a38a.

Skonnard A. 2003. Understanding SOAP. Microsoft Developer Network. March 2003. Available from: https://msdn.microsoft.com/en-us/library/ms995800.aspx. Accessed 2016 November 16.

Snowflake. 2015. Inside the snowflake elastic data warehouse. Snowflake Computing, Inc. Available from: https://www.snowflake.net/wp-content/uploads/2015/10/Snowflake_Inside_the_Elastic_Data_Warehouse_WP.pdf. Accessed 2016 November 16.

Stackflow.com. 2011. What exactly is the meaning of API? Available from: stackoverflow.com/questions/7440379/what-exactly-is-the-meaning-of-an-api. Stack Exchange Inc. Accessed 2016 April 22.

Sterling B, Gooch M, Dent B, Marenick N, Miller A, Sylvia G. 2015. Assessing the value and role of seafood traceability from an entire value-chain perspective. Compr Rev Food Sci F 14(3):205-68. Available from: http://onlinelibrary.wiley.com/doi/10.1111/1541-4337.12130/abstract.

Summer G, Kelder T, Ono K, Radonjic M, Heymans S, Demchak B. 2015. cyNeo4j: connecting Neo4j and Cytoscape. Bioinformatics 31(23):3868-69. doi:10.1093/bioinformatics/btv460.

Wenger-Trayner E, Wenger-Trayner B. 2015. Introduction to communities of practice. Wegner-Trayner. Available from: http://wenger-trayner.com/introduction-to-communities-of-practice/. Accessed 2016 November 21.

Willmes C, Kürner D, Bareth G. 2014. Building research data management infrastructure using open source software. Transactions in GIS 18:496–509. doi:10.1111/tgis.12060.

About the Global Food Traceability Center (GFTC)

The GFTC is assisting the global food industry to trace products through the supply chain to improve food safety, diminish risk, avert devastating health consequences, and economic loss to the food system. The GFTC serves all aspects of the food system by generating knowledge that addresses research gaps, and delivering applied research, objective advice, and practical expertise about global food product traceability and data collaboration for private benefit and public good.

GFTC Vision

To become the global resource and authoritative voice on food traceability.

GFTC Mission

To serve all aspects of the global food system by generating knowledge that addresses informational gaps while delivering applied research, objective advice, and practical expertise about food product traceability and data collaboration for private benefit and public good.

For the further information contact:

Global Food Traceability Center
Institute of Food Technologists
525 W. Van Buren, Ste 1000 Chicago, IL 60607
Phone: +1.312.782.8424 | Fax: +1.312.782.8348 | Email: info@ift.org
http://www.ift.org/gftc.aspx