Extensible Supply-chain Discovery Service Problem Statement

draft-rezafard-esds-problem-statement-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on July 18, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).
Abstract

This document discusses the requirements of an application layer protocol which can meet the needs of today’s complex and dynamic supply chains. Currently, supply chain communication traffic travels over the Internet using existing Internet protocols. This is a temporary solution for a growing niche. This document elaborates on issues that would arise if this trend continues. Also, this document outlines a set of design concerns that an application layer protocol needs to address in order to be deployable in a real-world supply chain.

Comments are solicited and should be addressed to the mailing list at esds@ietf.org and/or the author(s).
Table of Contents

1. Introduction ...................................................... 4
   1.1. Background ................................................. 4
   1.2. Terminology .............................................. 5
   1.3. Problem Statement ......................................... 5
   1.4. Description ............................................... 6
2. Internet Concerns .................................................. 7
   2.1. Public Networks and Tree-Walking Concerns ................. 7
   2.2. Bootstrapping Concerns .................................... 7
3. Objectives ........................................................ 9
   3.1. Resource Discovery ......................................... 9
   3.2. Client Query ............................................... 9
   3.3. Security .................................................. 9
   3.4. Access Control ............................................ 9
   3.5. Independence ............................................... 10
   3.6. Identifier Agnostic ....................................... 10
   3.7. Extensible ................................................ 11
   3.8. Retention Policy ......................................... 11
   3.9. Stale Links ............................................... 12
4. Technical Challenges ............................................... 13
   4.1. Auditability ............................................... 13
   4.2. Responsiveness .......................................... 13
   4.3. Availability ............................................. 13
5. Research Bodies .................................................. 14
6. Acknowledgements ................................................ 15
7. Contributors .................................................... 16
8. IANA Considerations ............................................. 17
9. Security Considerations ......................................... 18
10. References ..................................................... 19
    10.1. Normative References ................................... 19
    10.2. Informative References .................................. 19
Author’s Address .................................................... 20
Intellectual Property and Copyright Statements ..................... 21
1. Introduction

Supply chain Tracking System utilization is rising at an unprecedented rate. These systems enable tracking and tracing of physical objects as they move through a supply chain. Deployment of these systems has grown to a point that they can no longer operate effectively in isolation from other systems. There is a need to share data among these disparate systems, which are owned and operated by separate organizations.

1.1. Background

Traditionally supply chain communication has been routed over private network infrastructures. However in recent years this practice is abandoned in favour of communication over public networks. The communication and data exchange has taken the form of flat file data exchange, XML, and other proprietary forms across existing mechanisms, such as SFTP and SMTP. This method of exchange requires bilateral agreements and networking arrangements amongst all partners of a given supply chain. In this model, information sharing begins with the supply chain partner who provides lists of the objects (shipping manifest) that the other partners can expect to exchange within the supply chain. While this one way method is effective in very static supply chain relationships, its main drawback lies in inability to support dynamic routing of physical objects and, therefore, exception handling. For example, if an object arrived at supply chain partner C without prior notification from supply chain partner B or A, the product remains unidentified and not routable.

The advent of RFID tags has been a catalyst for the desire to reverse-lookup object information. Products are being tagged with RFID tags, traditional barcodes, and other types of proprietary object identifiers. The exchange of information now begins with the object and leads back to the supply chain partner. As the object is scanned at various key gates in the supply chain, a referral service must be available to match the object’s identifier either to a relevant supply chain partner or to a list of relevant supply chain partners and the data services that these partners offer to a requestor. This enables supply chains to route flexibly and handle exceptions.
1.2. Terminology

There are three actors in this problem:
Client: refers to an actor that seeks (sources of) information about an individual object.
Resource: refers to an actor that holds information about an individual object and may provide it to authenticated clients who satisfy some authorization criteria (access control policies and rules).
ESDS: refers to an intermediary lookup service that enables a client to locate one or more resources.

What emerges from combinations of these actors and their relationships are:
Partner: refers to a business entity which is comprised of Client and Resource actors belonging to an organization.
Supply chain: refers to a group of partners that have the desire to share information among themselves.

1.3. Problem Statement

Information sharing between partners is essential for all modern supply chain networks. There is a strict set of business and technical requirements that must be observed in order to enable open sharing of information in a supply chain.

There are resources and clients in each supply chain. Each resource wants to advertise its knowledge (data) to interested and authorized clients. Only deploying private networks to connect whole supply chains is no longer feasible, as the more efficient and economical means of connecting resources and clients is to use public network infrastructure. Currently, many supply chain track-and-trace initiatives are deployed on public networks and the information is routed through Internet. Because of this trend, it is highly desirable that a standardized protocol should be developed. An IETF standards process would ensure that the adopted protocol conforms to Internet’s operational needs.

A key principle of information sharing in the supply chain is that data ownership must be respected. This means that each partner can collect information within their organization and is not required to route that information to any other partner. However, they can choose to share selected information with other trusted partners. This in turn means that the complete lifecycle information about any individual object may be held by multiple resources throughout the supply chain or the product lifecycle. Therefore a mechanism is needed in order to facilitate the gathering of this information.
A key requirement is that information accessibility is fully controllable. The confidential information must be secure and hidden from unauthorized-clients and only visible to the intended-clients in a supply chain. Unauthorized clients need to be barred from viewing, eavesdropping, or deducing information, in order to establish trust and reputation with the participating resources.

There must be a common set of data that all resources will offer. This set must be defined and agreed upon in the final protocol. This set may include data such as object identifier, lifecycle step, bootstrap location, links to back-end systems. An essential feature is for the protocol to be extensible beyond the common data set to facilitate the needs of supply chains that discover additional uses.

Defining a bootstrapping procedure is a necessity when designing a global and autonomous network of systems. Currently there are deployed supply chain systems that bootstrap via Internet’s DNS roots. One example of this is the EPCglobal Object Name Service (ONS). While ONS enables an economical means of bootstrapping, improper implementations may increase the traffic on DNS roots exponentially. Since data will be routed through the Internet, the bootstrapping procedure needs to be formulated under the IETF standards process.

1.4. Description

An Extensible Supply-chain Discovery Service (ESDS) provides a mechanism to locate one or more sources of information about an individual physical object. This may include the original manufacturer or supplier of the object, as well as other organizations who have handled the object at some point during its lifecycle (including repair and maintenance organizations) and even organizations (such as customs agencies) who might hold information records related to the object, even though they may have never had physical custody of the object.

This document defines the Problem Statement, Objectives and Technical Challenges related to the application layer protocol currently proposed as Extensible Supply-chain Discovery Services (ESDS). ESDS captures and queries historical events related to specific objects with attached object identifiers. The interface enables disparate applications to track-and-trace shared lifecycle views of object identifiers across a supply chain. Additionally, ESDS provides referral services in a loosely coupled mechanism with granular security that enables selective visibility.
2. Internet Concerns

2.1. Public Networks and Tree-Walking Concerns

Currently, another standards body, EPCglobal, has issued a related standard referred to as ONS (Object Naming Service, 1.0). ONS is effectively an extended version of DNS that does not benefit from the IETF review process and, by design, necessitates increased tree-walking. ONS specifies a reverse mapping of the EPCglobal "SGTIN" (one type of supply chain object identifier) as a domain and allows for a reference (i.e. URL) to a manufacturer’s relevant back-end system (using a NAPTR record). The SGTIN identifier is comprised of an EPC Manager Number, an Object Class, and a Serial Number. The ONS lookup excludes the Serial Number portion of the SGTIN. However, the ONS specification has already been extended in industry pilot projects to include the Serial Number, as this enables item level lookups for tagged objects in the supply chain. Using serial level lookups, ONS could be used to indicate point to point referrals through the passage of a relevant identifier throughout the supply chain. This would require successive updates to the hierarchal ONS to indicate incremental supply chain partner referrals, reducing the effectiveness of caching. Alternatively the ONS could provide a single, static point of referral to the first or initiating supply chain partner. However, even a relatively static entry, which only refers to the point of origin within the supply chain, would drive the number of public zone entries to extremely large numbers if an individual record were created for each serial number. One common suggestion to manage this problem is that multiple alternate ONS roots can be managed for separate and unrelated supply chains and/or regions. However, since there is nothing to prevent ONS from operating in the existing Internet root hierarchy, even alternate ONS providers can opt to drive traffic to the existing Internet root servers, rather than operate their own ONS roots. There has already been a pilot ONS implementation under the .aero zone (sgtin.id.ons.autoid.aero) where this phenomenon may already be observed. ESDS must aim to prevent this problem by keeping most of the network traffic off the Internet root hierarchy.

2.2. Bootstrapping Concerns

Currently there are discussions on how to best facilitate a bootstrapping process for objects in the supply chain. The bootstrapping process involves locating an object’s Discovery Service server by an interested and authorized client. The bootstrapping process needs to be enabled with only the information provided by the object identifier. Unlike DNS, where there is a known set of root servers, ESDS will have numerous roots for various supply chains operating globally. This, in turn, complicates the bootstrapping
A common bootstrapping scenario is exception handling. For example, if an object is mis-delivered, a recipient who has no pre-existing relationship to the supply chain, needs to obtain object ownership information and its corresponding Discovery Service server. ESDS design must aim to accommodate this scenario while respecting privacy and security considerations.

It has been suggested to use the ONS for the bootstrapping process. However, ONS’s hierarchical identifiers have raised privacy and security concerns by multiple participants in the supply chain. While ONS can technically support multiple identifier schemes, with multiple issuing authorities, its hierarchical operation does depend on structured identifiers (for example, ManagerNumber.ObjectType.SerialNumber). These identifiers leak information about products such as type and manufacturer and as a result could compromise the privacy of an individual transporting them. Additionally, ONS has no authentication or access control. ESDS must be designed for serial level lookups and must support unstructured opaque identifiers to use as lookup keys within an ESDS service. It should fully support authentication and object level access controls to address privacy concerns.

To facilitate bootstrapping and exception handling scenarios ESDS design could consider a peer-to-peer lookup protocol such as XMPP. This would keep the ESDS traffic flat and avoid walking up the Internet root hierarchy. A major concern is that the bootstrapping design must not implicitly establish monopolies in the long run. The IETF process will ensure that the resulting protocol design addresses the concerns of all participants in the global supply chain.
3. Objectives

This section outlines the objectives of the ESDS protocol. In efforts to convey the goal of each objective, example solutions are provided. These solutions are provided to trigger discussion on the subject matter, and are not intended to be the suggested solution to fulfil the objective.

3.1. Resource Discovery

An ESDS must provide a mechanism whereby a resource can dynamically establish a link for an individual object (or range or class of objects) that points from the ESDS to the resource. The link can be expressed as a string or URI and it is helpful if this is accompanied by an indication of the type of service which can be accessed via the link (in order to distinguish between web pages, web services, EPC Information Services (EPCIS) and other communication mechanisms which might even include phone or fax numbers).

3.2. Client Query

An ESDS should provide a mechanism whereby a client can query the ESDS in order to retrieve a list of links to one or more resources. Queries may be one-time queries or standing queries, and an ESDS may support either type of query, or both.

The query interface needs to define the criteria fields as well as acceptable criteria values, such as regular expressions or wildcards.

3.3. Security

Since ESDS needs to be deployable over public network infrastructure, issues of security and privacy are of heightened importance. Clients must be authenticated to prevent theft of information and resources must be authenticated to ensure integrity of information. The information routed over the Internet must be encrypted. It is suggested that the security model be based on open standards, trusted by the supply chain industry.

The ESDS protocol should be decoupled from the security layer and not have embedded components specific to certain security protocol implementations. This will enable ESDS implementations to respond quickly to changes in the ever advancing security layer protocols.

3.4. Access Control

An ESDS should provide a resource with the ability to protect its link information in order to retain control over which clients are
allowed to read this information. Such rules may be expressed in the form of access control policies which are evaluated against the client’s authentication credentials and its role in relation to the provider of the resource, as well as other criteria such as the time elapsed since the link was created.

The situation may arise where a client and the provider of a resource have no existing trust relationship with each other. An ESDS should allow a resource to specify multiple levels of ‘visibility’ to such a client, so that the resource either remains completely ‘silent’ or ‘invisible’, or so that an opaque handle is visible. The opaque handle should not reveal the identity of the resource in any way, but may be used to facilitate the initial negotiation between a client and a resource, if an ESDS or associated service provides such a mechanism, such as forwarding a number of messages from the client to the provider of the resource, provided that the client specifies the handle in their message. To protect the resource provider and ESDS from additional burden, such a facility may be limited in the number of messages which are forwarded and the time window following the client’s query during which forwarding of messages is offered.

3.5. Independence

In today’s morphing supply chains there will always be resources that cannot or will not participate in track-and-trace efforts. If a resource in a supply chain chooses not to participate, the protocol architecture needs to be tolerant of this missing link in the supply chain. The only acceptable consequence of a non-participating resource would be to miss the information that would have been supplied had it participated.

3.6. Identifier Agnostic

To enable grouping of information belonging to the same object, each object needs to be uniquely identifiable as it moves through the supply chain and its lifecycle steps. The protocol cannot safely rely on unique object identifiers alone, because an identifier may enter the supply chain multiple times. One use case for this is returnable bins, where the same bin will go through the supply chain many times. Another use case is airline baggage, where the same baggage identifier could appear the following year, because the identifier is only required to include a Julian date (the day of the year) but is not required to include the year.

As an object moves through the supply chain, it produces events of interest. The same event on the same object may take on a different meaning depending on the lifecycle step of the object. These events would be more useful to the interested partners if they conveyed some
information on the lifecycle step of the object being tracked. The lifecycle defined by a supply chain should enable intelligent exception handling by a partner’s Business Application. Also a lifecycle definition should facilitate re-using of the same object identifier in a supply chain. A possible solution could include the combination of a non-unique identifier with an unique lifecycle identifier. This would require consideration as to how the downstream partners might know the lifecycle identifier in order to add additional events of interest.

3.7. Extensible

The event data needs to accommodate various supply chains and their business requirements. Therefore it must be an extensible protocol which enables the partners to communicate messages specific to their group and supply chain.

An ESDS protocol should enable sharing of information and refrain from involving the business rules of supply chains. This will keep the interface clean and uniform across all supply chains and ESDS services.

3.8. Retention Policy

The retention time for data records in ESDS would vary based on the supply chain’s business and regulatory requirements.

- For tracking of shipments, the records might only need to be stored while the shipment is in transit and has not yet reached its final customer (e.g. a few days to a few weeks)
- For some objects (e.g. consumer goods/retail sector), the primary interest may be tracking from manufacturer to point of sale (e.g. a few days to a few months)
- In some sectors (e.g. pharmaceuticals), regulatory guidelines may require records to be retained for several years beyond the point of dispensing.
- In other sectors (e.g. aerospace parts), the lifecycle up to the point of delivery is only the initial phase of the lifecycle of the part - and there may be significant interest in tracking the part (and its sequence of custodians and information providers) throughout its active service life, which can be up to 30 years for some parts.

So the protocol needs to facilitate defining and customizing these retention policies in the supply chains.
3.9. Stale Links

There are situations where the link information (such as a URL) that was originally specified is no longer effective (e.g. because the provider of the resource has not taken care to maintain redirection from the original link address to the new location of the resource when restructuring a website or moving to a different domain name). In such situations, it is desirable that an ESDS can provide a client with link information that is current and effective. For audit purposes, it may also be necessary for an ESDS to be able to retain and reconstruct the original (or previous) link information, even if it is no longer effective.

This may also imply that an ESDS should allow a resource provider to loosely couple the link record or event with the current link address, to ease migration of multiple records to a new link address, while providing a mechanism to recover a full audit trail of such changes of link addresses.
4. Technical Challenges

4.1. Auditability

Based on some supply chain business and regulatory requirements, auditing capabilities should be facilitated by ESDS to provide accountability if and when something goes wrong. With an auditing mechanism, record data can be tracked and the person responsible identified, thus a series of data records can be reconstructed at a later date, allowing the supply chain to prove who was responsible for which data records [bridge-security-analysis].

4.2. Responsiveness

ESDS implementations will need to be designed to accept updates in a close to real time basis from multiple providers of information across the supply chain or lifecycle of an object (including organizations that handle the object beyond the point of sale or delivery, e.g. for repair purposes, maintenance, returns and reverse logistics, as well as recycling, remanufacturing and other end-of-life processes). Because they store serial-level records, they will need to be sufficiently scalable to store large volumes of data, possibly up to trillions of records per year.

4.3. Availability

ESDS availability requirements would vary from supply chain to supply chain. Research by BRIDGE shows that the uptime requirements for some supply chains are 99.99% year round.

It is expected that the ESDS instances will be available over a shared network that exposes them to the effects of network attacks. Furthermore, in many cases it is expected that these components should be globally reachable from the Internet and not hosted on a secure private network. Such components are also built using commonly available Operating Systems and middleware (e.g. Application Servers). Thus they are also subject to any vulnerabilities of these supporting systems.

A major security issue for shared services such as the ESDS or ONS is service availability. In particular if you consider services that are vital for supply chain processes (e.g. "pharma ePedigree" or "product-authentication") ESDS needs to be able to guarantee minimal amount of service downtime due to security vulnerabilities and attacks [bridge-security-analysis].
5. Research Bodies

Currently, the standards organization EPCglobal, and EU research projects BRIDGE, SMART, and PROMISE are looking into the global supply chain track-and-traceability challenge. As part of their research, each of them has identified the need for Discovery Services to link resources and clients in the supply chains.

EPCglobal is beginning to gather user requirements for Discovery Services. However, EPCglobal is a paid membership organization focused on serving their own subscriber community. Although the final ratified EPCglobal standards are open and freely available to download, the subscription fees for joining the EPCglobal community may deter the greater proportion of the global supply chain community from directly participating in the development of their global standards.

IETF would be the ideal standards body to oversee the development of this protocol because of its deep knowledge of Internet infrastructure and experience with development of application layer protocols.

An IETF working group would be an inviting and open community which facilitates contribution and participation of all interested parties involved in the global supply chain. Unlike an EPCglobal work group, there would be no economic barriers to participation in the development of the technical standard. The output would be released as a freely available RFC in the public domain.
6. Acknowledgements

This document and the process of authoring was made possible by the excellent xml2rfc tool [RFC2629]. Credit must also be given to Scott Hollenbeck author of [RFC4930] for the organization and grouping of RFC sections.
7. Contributors

Dr. Mark Harrison
Senior Research Associate, Distributed Information and Automation Laboratory
Director, Auto-ID Labs at Cambridge
Institute for Manufacturing
University of Cambridge
Mill Lane
Cambridge, UK
CB2 1RX

Phone: +44-(0)1223-338178
Email: mark.harrison@cantab.net

Michael Young
Senior Director, Technology
Afilias Canada
204-4141 Yonge Street
Toronto, ON M2P 2A8
CA

Phone: +1-416-646-3304
Email: myoung@ca.afilias.info
8. IANA Considerations

This document has no actions for IANA.
9. Security Considerations

This document is a problem statement that does not by itself introduce any security issues.
10. References

10.1. Normative References


10.2. Informative References


Author’s Address

Ali Rezafard
Afilias Canada
204-4141 Yonge Street
Toronto, ON M2P 2A8
CA

Phone: +1-416-646-3304
Email: arezafar@ca.afilias.info