A Secure Platform for Information Sharing in EPCglobal Network

Jie Shi[a,b] Yingjiu Li[a] Robert H. Deng[a] Wei He[c] Eng Wah Lee[c]

[a]*School of Information Systems, Singapore Management University*
[b]*Jinan University, China*
[c]*Planning and Operations Management,*
Singapore Institute of Manufacturing Technology

Abstract

With the rapid development of RFID technology, the EPCglobal network has drawn considerable attention from both research and industry communities, which enables supply chain partners to automatically share information and improve the visibility of supply chains. As the information shared in the EPCglobal network is usually sensitive and valuable, security mechanisms should be provided. In this paper, we aim at designing and implementing a secure information sharing platform in the EPCglobal network with a focus on authorization mechanism. We also design and implement a track and trace application based on the proposed secure platform so as to demonstrate its feasibility and practicality.

1. Introduction

With the rapid development of Radio Frequency Identification (RFID) technology, RFID-enabled supply chain networks have drawn considerable attention from both research and industry communities [1-3]. As an industry standard of RFID-enabled supply chain networks, the EPCglobal network is designed with the intention of increasing visibility of objects within supply chains [4]. The EPCglobal network consists of the following components: EPC tags, RFID readers, Application Level Events (ALE) interface, EPC Information Service (EPCIS), EPC Object Naming Service (EPCONS) and EPC Discovery Service (EPCDS) [4]. In the EPCglobal network, each physical product is associated with an RFID tag, represented by a unique Electronic Product Code (EPC). This EPC can be retrieved from an RFID tag wirelessly via an RFID reader without contact-of-sight. An EPC code and associated event information are usually processed by a middleware (ALE), and stored locally at each supply chain partner's EPCIS [5]. EPCDS and EPCONS are designed to locate EPCIS systems, from which users can obtain the addresses of EPCIS systems which store the detailed event information about a given EPC of interest. EPCDS and EPCONS facilitate the information sharing among distributed EPCIS systems. EPCIS, EPCDS and EPCONS are collectively called EPCglobal network services, which constitute an information sharing platform for the EPCglobal network.

However, to the best of our knowledge, there is still a lack of integrated prototypes for the EPCglobal network services so far due to many challenges such as high cost, lack of standards for EPCDS, security and privacy issues, information sharing issues, and voluminous data issues [6]. Among them, the security and privacy issues and the lack of EPCDS standards are the most significant challenges. As the information stored and shared in EPCglobal network is usually very sensitive (which may reveal inventory level, trading partners, and business plan), the security and privacy concerns thwart a widespread adoption of the EPCglobal network [2]. Even though there is a large body of research work on the security and privacy aspects of communications between RFID tags and readers, the security and privacy issues on the EPCglobal network services (EPCDS, EPCIS and EPCONS) have not been rigorously studied [7,8]. However, as the information stored and shared in the EPCglobal network services is usually valuable and sensitive, supply chain partners hesitate to use the EPCglobal network without adequate security and privacy protection mechanisms. Therefore, it is important to address the security and privacy concerns in the design and implementation of the EPCglobal network services. In particular, we need to design and implement a secure and efficient

EPCDS which is a search engine in the EPCglobal network. EPCDS helps users locate EPCIS systems so as to share information among different EPCIS systems. Without EPCDS a full visibility of objects in supply chains cannot be realized.

In this work, we aim to design and implement a secure platform for information sharing in the EPCglobal network. We have three primary goals, namely 1) facilitating global information sharing among supply chain partners; 2) supporting authorization mechanisms in EPCglobal network services; 3) reducing the cost of managing and maintaining supply chain partners' data and authorization policies. For facilitating global information sharing among supply chain partners, an EPCDS server is designed and implemented. We implement an EPCDS server without considering EPCONS because the latter provides search services at class-level only while EPCDS provides query services at item-level [4]. In order to protect supply chain partners' data in EPCglobal network services, EPCIS and EPCDS are both extended to support authorization mechanisms such that supply chain partners can define access control policies in EPCIS and EPCDS systems so as to specify which users are allowed to access their data. As authentication is prerequisite of authorization, an authentication mechanism is enabled in our implementation. We observe that both data and authorization policies in EPCDS are subsets of those in EPCIS systems. In order to reduce the cost of managing and maintaining supply chain partners' data and authorization policies, we provide a choice so that supply chain partners can automatically publish data and authorization policies into EPCDS from their EPCIS systems. In summary, the major contribution of this paper includes the design and implementation of secure EPCIS, EPCDS, as well as a secure track and trace application, which demonstrates the feasibility and practicality of building a secure platform for information sharing in EPCglobal network.

The remainder of this paper is organized as follows. Section 2 gives the background and related work of our research. Section 3 presents the design of a secure prototype for EPCglobal network services. The implementation detail of the prototype is given in Section 4. Section 5 presents a discussion of the proposed prototype. A track & trace application is described in Section 6. Section 7 concludes the paper.

2. Background and Related work

2.1. EPCglobal Network

As an industrial standard of RFID-enabled supply chain networks, the EPCglobal network provides a platform for supply chain partners to share product information [4]. After registering into the EPCglobal network, supply chain partners can publish event information of products into the EPCglobal network and share the information with others in internet. The event information can be used to enhance the visibility of the location and movement of objects within supply chains.

The architecture of the EPCglobal network is described in a standard document [4]. Figure 1 illustrates the EPCglobal network, including EPC Discovery Service (EPCDS), EPC Information Service (EPCIS), EPC Object Naming Service (EPCONS) and an RFID sub-system, where the RFID sub-system consists of RFID tags and readers.

In the EPCglobal network, each component plays a unique and important role. The RFID sub-system is in charge of capturing event information when physical objects move across different companies, e.g., manufacturers, suppliers and retailers. The event information is processed and delivered to EPCIS systems via Application Level Events (ALE) interface. EPCIS mainly contains two major components: EPCIS repository and EPCIS query interface. The delivered event information is stored in the EPCIS repository and accessed by end users through the EPCIS query interface. Usually, each company has its own RFID sub-system and an EPCIS system, which enable information sharing in a local domain. In order to support global information sharing within a supply chain network, EPCONS and EPCDS are introduced in the EPCglobal network[2], so that a full visibility of supply chains can be realized.

EPCDS and EPCONS are both designed to help users locate EPCIS systems which store detailed events information. EPCONS is designed following the existing internet Domain Name System to locate EPCIS systems while EPCDS works as a search engine. The mainly difference between EPCONS and EPCDS is that, while EPCDS provides query services for item-level information, EPCONS provides search services for class-level information only. EPCDS is more powerful and useful than EPCONS in locating EPCIS systems. Therefore, we focus on EPCDS instead of EPCONS in this paper.

2.2. EPC Discovery Service

EPC Discovery Service (EPCDS) is the search engine for the EPCglobal network, allowing users to find EPCIS systems which store detailed event information about EPC of interest. According to previous research work, there are three different models for EPCDS: directory model, relay model and aggregating model [10].

2. To date, except for the standard of EPCONS, there is still no standard of EPCDS released so far [4].

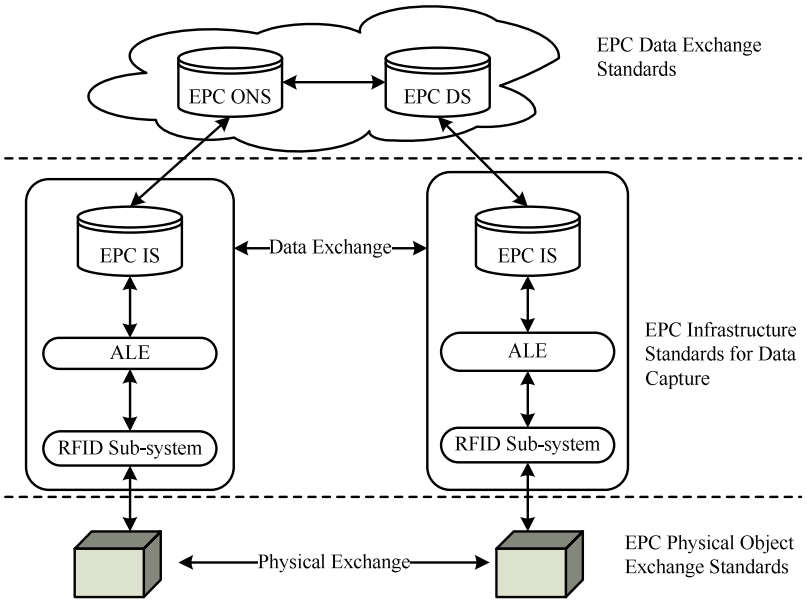

Figure 1. Architecture of the EPCglobal network [9].

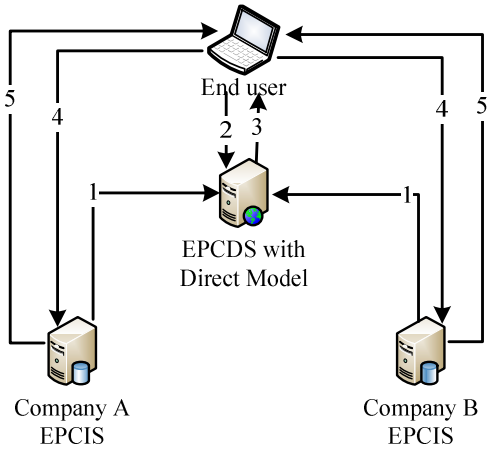

Figure 2. Information flow in EPCglobal network services with EPCDS supporting directory model

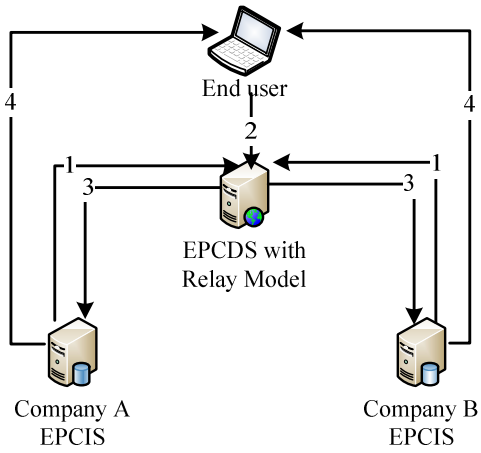

Figure 3. Information flow in EPCglobal network services with EPCDS supporting relay model

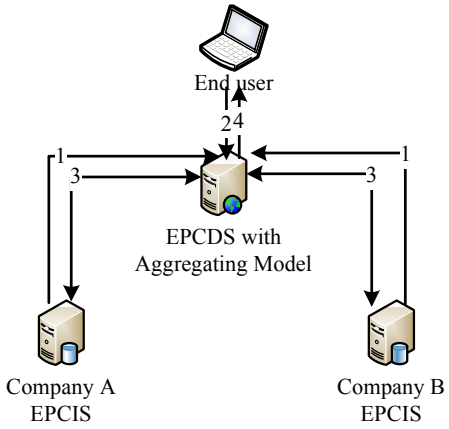

Figure 4. Information flow in EPCglobal network services with EPCDS supporting aggregating model

In the directory model, the EPCDS system manages a directory of EPC and corresponding EPCIS systems' addresses. The information flow in EPCglobal network services with EPCDS supporting the directory model is shown in Figure 2. When a product attached with an RFID tag is processed by a supply chain partner, the corresponding event information is collected via the partner's RFID sub-system and transmitted to its EPCIS system. When the EPCIS system receives the event information about an EPC tag for the first time, it notifies an EPCDS system that it has the detailed event information about this EPC (line 1 in Figure 2). When a user searches for the information about a product with a given EPC, he first issues a query to the EPCDS to obtain the addresses of EPCIS systems which have the detailed information about this EPC (lines 2 and 3 in Figure 2). Next, the user queries each EPCIS system respectively using the addresses returned by the EPCDS for the detailed event information (lines 4 and 5 in Figure 2).

In the relay model, the EPCDS system does not return the addresses of EPCIS systems immediately upon request. Instead, it redirects the query request to corresponding EPCIS systems. The information flow in this case is shown in Figure 3. Similar to the directory model, EPCIS system notifies the EPCDS system that it has the detailed event information about an EPC tag when it receives the event information about this EPC for the first time. When a user searches for the information about a given EPC, a query is sent to the EPCDS system, which redirects the query to the corresponding EPCIS systems. Finally, these EPCIS systems return the query result directly to the end user.

The third model, the aggregating model operates similar to the relay model. The difference is that, instead of returning EPC event information directly to a user, each EPCIS system returns the result back to EPCDS, which aggregates the information returned from EPCIS systems before sending the aggregated result to the end user. The information in this case is shown in Figure 4.

As the directory model, the relay model and the aggregating model satisfy different users' requirements, we consider all three models in our design and implementation.

2.3. Related Work

In order to improve supply chain visibility, RFID-enabled supply chain network has drawn considerable attention from research and industrial community in recent years. Many track & trace systems are designed and implemented in the past decade, including IBM Theseos, DIALOG, and the system developed in BRIDGE project [3]. However, the problem of sharing supply chain information among different partners is still a challenging problem. A standard supply chain network, the EPCglobal network, is proposed to address this problem.

To increase supply chain visibility, much related work has been focusing on the design and implementation of track & trace systems in the standard EPCglobal network [1, 5, 11]. However, the security and privacy problems have not been rigorously addressed in these works.

Recently, many security mechanisms are proposed to protect different components of the EPCglobal network, including EPCIS, EPCONS, and EPCDS. For EPCIS, a fine-grained access control mechanism is proposed and implemented [12]. For EPCONS, a peer-to-peer name service architecture is proposed to enhance the data security of EPCONS and the privacy of the users [13]. However, this work is based on peer-to-peer system which does not fully conform to the EPCglobal network standards. Following to the work of EPCONS, a privacy-enhanced discovery service is proposed to protect the privacy of users in EPCDS system [14], which is also based on peer-to-peer system. In [15], Yan et. al.

consider an different situation where the EPCDS system is untrusted, and they propose a pseudonym-based design to mitigate potential attacks. Their work does not conform to the standard EPCglobal network either and it is not practical in real world applications due to high overhead of converting EPC to pseudonyms. In [16], Shi et. al. proposed a secure track and trace system, in which they proposed a new approach to enhance the security of EPC discovery service system based on the relay model. However, as they mentioned, the EPCDS system and EPCIS system in their work do not fully conform to the standard EPCglobal network.

Rigorous effort has been made in the research community on the security and privacy aspects of RFID systems [17]. However, these works mainly target at RFID communication systems, rather than EPCglobal network. Since the information shared in EPCglobal network is sensitive and valuable (e.g. inventory level, trading partners, and trading volumes), it is critical to address the security and privacy concerns in EPCglobal network. This is the focus of this paper.

3. Secure Prototype for EPCglobal Network Services

We design a secure platform for information sharing in EPCglobal network in this section.

3.1. Architecture of Secure EPCglobal Network Services

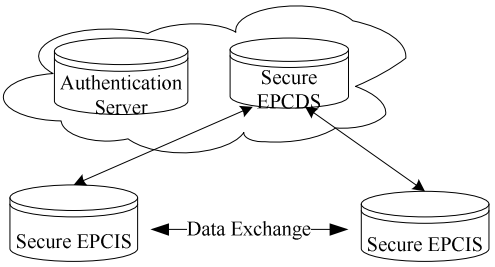

Figure 5. Architecture of Secure EPCglobal network Services

The architecture of secure EPCglobal network services is shown in Figure 5. Different from the standard EPCglobal network services, an authentication server is added and the secure EPCDS and the secure EPCIS are used to replace the original EPCDS and EPCIS. The authentication server is designed to authenticate users in the whole EPCglobal network services. As there exists some work on authentication in EPCglobal network [4,7], we mainly focus on authorization in this paper. Different from the original EPCDS and EPCIS, both secure EPCDS and secure EPCIS support authorization to protect supply chain partners' data with access control policies.

3.2. Secure EPC Information Service

In the EPCglobal network, EPCIS is responsible for collecting event information from the filtering and collection middleware (ALE), and making these information available to authorized users. EPCIS is composed of an EPC repository and two standard interfaces, namely Capturing Interface and Query Interface. The Capturing Interface collects EPC event information from underlying application whilst the Query Interface allows users to retrieve event information.

In the standard document on EPCIS, the security issues such as authentication and authorization are not fully addressed even though it is stated that authentication and authorization mechanisms should be implemented in EPCIS.

We design a secure EPCIS (SecEPCIS) as an extension to the standard EPCIS. SecEPCIS consists of two primary functionalities as shown in Figure 6, i.e., data management and authorization management. Date management operates with four sub-functionalities, namely data storage, data capture, data query and data publish. The former three sub-functionalities are the same as in the standard EPCIS while the data publish is newly designed to allow SecEPCIS to automatically publish data into EPCDS for the purpose of reducing the data management cost of supply chain partners. Authorization management is introduced to allow supply chain partners to control the accesses to their data. It operates with the following four sub-functionalities: policy storage, policy publish, policy management and access enforcement. Policy storage is in charge of storing the access control policies specified by supply chain partners; policy publish provides an option for supply chain partners to publish access control policies to EPCDS automatically; policy management is provided for supply chain partners to create, modify and delete their access control policies; finally, access enforcement is in charge of controlling users' accesses under the access control policies defined by supply chain partners.

Following the functionalities given above, we design SecEPCIS as shown in Figure 7. SecEPCIS is made up of the following components: Enforcement, Data Storage, Data Publish, Policy Service, Policy Management, Policy Storage, Policy Transformation, and Policy Publish. In SecEPCIS, there are three kinds of interfaces, i.e., Query Interface, Capture Interface, and Policy Interface. In the following, we will describe how these components work together to achieve the functionalities of data capture, data query, data publish, and authorization.

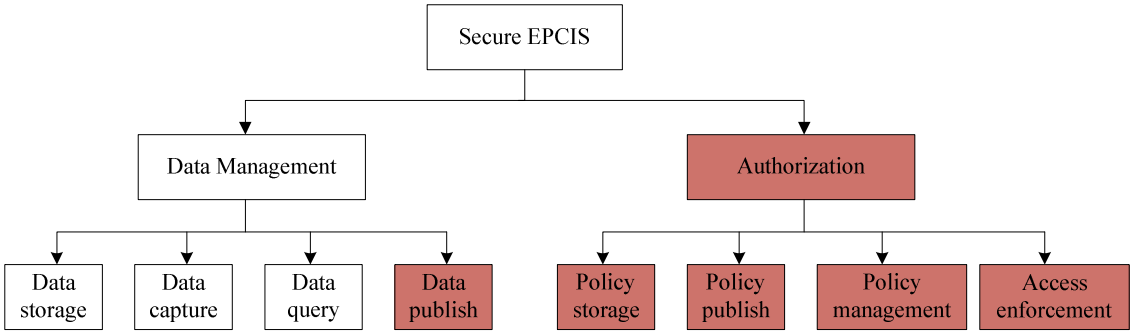

Figure 6. Functionalities of Secure EPCIS

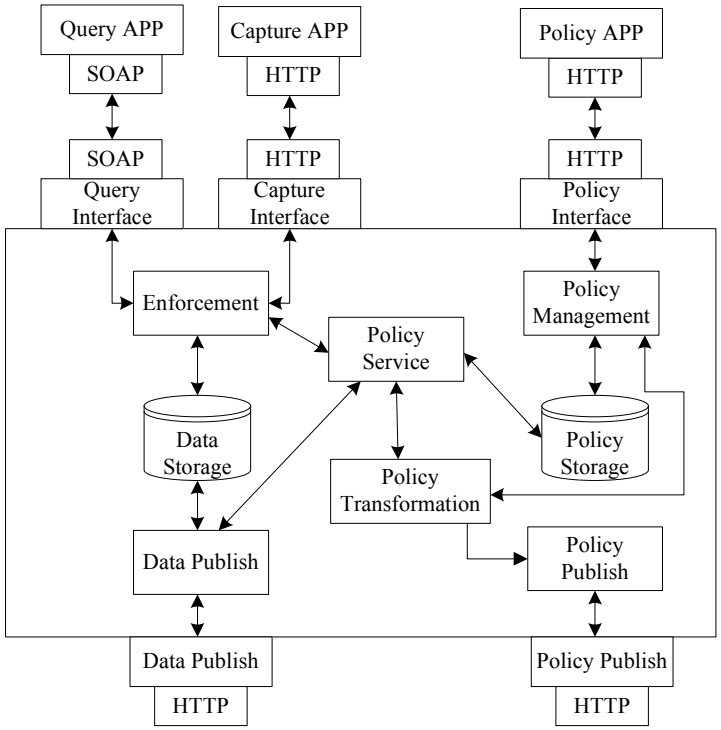

Figure 7. Architecture of secure EPCIS

Data Capture. The filtering and collection middleware (i.e., ALE) publishes event information into SecEPCIS through the capture interface. SecEPCIS stores the event information in the Data Storage component. There is no difference between the capture interfaces of standard EPCIS and SecEPCIS. We do not provide any access control mechanism for capturing operation in SecEPCIS, as the operation happens in the domain of one supply chain partner, and we focus on the information sharing among different partners in this paper. Nonetheless, it is easy to implement an access control mechanism for data capture operation in a way similar to data query as stated below.

Data Query. End users retrieve data from SecEPCIS through the query interface. After registering in the EPCglobal network, each user can submit queries to SecEPCIS through the query interface. When receiving a query from a user, the Enforcement component first authenticates the user and checks the integrity of this query. If both authentication and integrity check pass, the Enforcement component requests Policy Service to provide corresponding access control policies for this user. Policy Service searches for corresponding policies in the Policy Storage component, combines policies if multiple policies exist, and sends the combined policy back to Enforcement component. After receiving the combined policy, the Enforcement component processes the user's query under the control of the policy. Finally, the query result is sent to the user by this SecEPCIS.

Data publish. SecEPCIS can automatically publish data into EPCDS so that the management

cost of supply chain partners is reduced. If supply chain partners allow their SecEPCIS systems to automatically publish data into EPCDS, SecEPCIS retrieves data from the Data Storage component, filtering and publishing these data accordingly. SecEPCIS may also record certain auxiliary information such as which data has been published.

Authorization. Supply chain partners manage access control policies through policy interface. With the policy interface, supply chain partners can define, modify and delete access control policies according to their security requirements. Take the creation of access control policy as an example: after receiving an access control policy, the Policy Management component first checks the syntax and sematic of the policy, processes the policy and stores it in Policy Storage if everything is normal. Another choice for a supply chain partner is to publish access control policies into EPCDS automatically. In this case, the newly created access control policy for SecEPCIS is sent to Policy Transformation component, which modifies the policy into access control policies suitable for EPCDS. The modified policies should be in accordance with the original policy defined by the supply chain partner. Finally, the modified policies are sent to the Policy Publish component and further published to EPCDS. The management of access control policies becomes easier for supply chain partners if they choose to automatically publish access control policies to EPCDS. The data publish and policy publish components help reduce the cost of supply chain partners and ease the adoption of EPCglobal network.

3.3. Secure EPC Discovery Service

The EPCglobal network is designed to support visibility of supply chains [4]. As an important part of EPCglobal network, EPCIS allows supply chain partners to exchange item-level information with each other provided that it is known which EPCIS systems have the item-level information about a given product. EPCDS is designed to provide a complementary lookup mechanism to enable supply chain partners to locate EPCIS systems for the item-level information of interest. In other words, EPCDS is a search engine in EPCglobal network which enables global item-level information sharing among supply chain partners.

To protect supply chain partners' index information in EPCDS, a secure EPCDS (SecEPCDS) is designed and implemented. Two primary functionalities in SecEPCDS are shown in Figure 8, namely data management and authorization management. Data management contains three sub-functionalities, including data storage, data publish and data query, while authorization management includes policy storage, policy management and access enforcement.

The system architecture of SecEPCDS is shown in Figure 9. SecEPCDS consists of the following components: enforcement, date storage, aggregation, policy service, policy management, policy storage, relay query, query interface, publish interface, and policy interface. In what follows, we describe how these components work together to achieve the functionalities of data publish, data query and authorization.

Data publish. Supply chain partners publish data into SecEPCDS through the publish interfaces of their EPCIS systems. After receiving a data publish request, the enforcement component first authenticates the user, and checks the integrity of this request; next, it requests the policy service component to retrieve and combine corresponding access control policies; then, it processes the request under the control of the received policy. Finally, the published data is stored in the data storage component.

Data query. There are three types of queries in SecEPCDS: abstract query, aggregating query and relay query. For abstract query, the procedure is similar to data publish. The enforcement component first authenticates a user and checks the integrity of a request; then it requests the policy service to provide the combined policy; finally it enforces the query under the control of the received policy and returns the result to the user. For aggregating query, SecEPCDS first executes the abstract query and obtains the addresses of EPCIS systems which have the detailed event information about the EPC submitted by the end user; then it sends the query and these addresses to the aggregation component. After receiving the request, the aggregation component requests relay query component to further retrieve the detailed event information from the corresponding EPCIS systems. After receiving the detailed event information, the aggregation component aggregates and returns the result to the user. The enforcement of relay query is similar to aggregating query, except for that SecEPCDS does not require the corresponding EPCIS systems to send query result back to it, instead, it requires them to send query result to the end users directly.

Authorization. Similar to the authorization of SecEPCIS, supply chain partners can manage their access control policies through the policy interface in SecEPCDS. For example, after receiving policy creation request, the policy management component authenticates the user, checks the integrity of this request, processes the policy and stores the policy in the policy storage component.

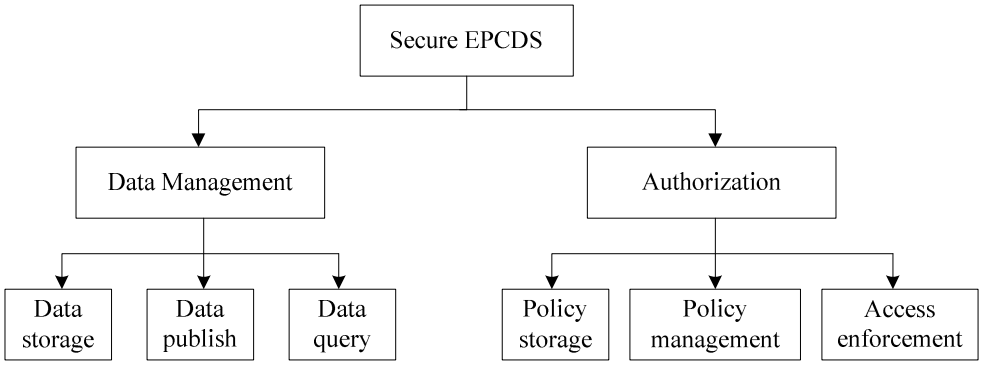

Figure 8. Functionalities of Secure EPCDS

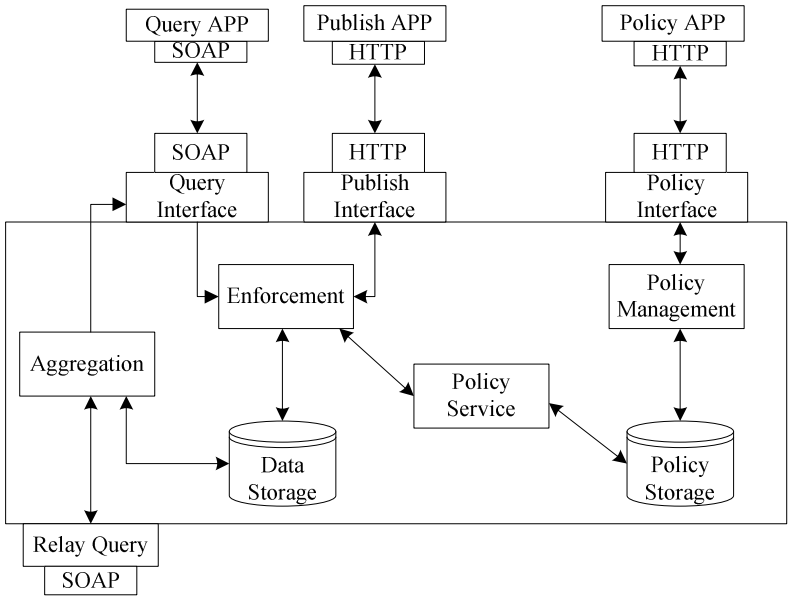

Figure 9. Architecture of Secure EPCDS

4. System Implementation

In this section, we provide implementation details for the secure platform we designed in EPCglobal network.

Following the recommendations from GS1 [4] and a related paper [7], our authentication server supports X.509 public key infrastructure (PKI) and password-based authentication as widely used in real world applications.

We use attribute-based access control to secure EPCglobal network services, including SecEPCIS and SecEPCDS. An attribute-based access control policy is specified based on the attributes of subjects and objects as widely used in distributed systems [18]. In EPCglobal network, each supply chain partner has the flexibility to decide what access control policies to use in protecting its data in EPCIS and EPCDS. However, traditional access control models, such as discretionary access control (DAC), mandatory access control (MAC) and Role-based access control (RBAC) [18,19], are too restrictive and not flexible enough for EPCglobal network. Therefore, we design and implement an extended attribute-based access control for EPCglobal network services. The following example shows that traditional attribute based access control (which is more generic than DAC, MAC, and RBAC) cannot be applied directly due to specific security requirements in EPCglobal network.

Example 1. Suppose that there are three supply chain partners in the EPCglobal network: Manufacturer M1, Distributor D1 and Retailer R1. They collect detailed event information and store it in their EPCIS systems. They also send index information to an EPCDS system. They define the following security policies to protect their EPC data:

- *P1* (defined by M1): Information about any product handled after 2011-01-01 can be accessed by supply chain partners who have

handled this product and are distributor companies.

- *P2* (defined by D1): Information about any product whose EPC is urn:epc:id:404958810:* can be accessed by supply chain partners who have handled this product after D1 handles it.
- *P3* (defined by R1): Information about any product handled after 2011-03-01 can be accessed by supply chain partners who have handled this product before R1 handles it.

In the above example, these security requirements cannot be specified using traditional attribute-based access control directly due to the term "who have also handled this product" in security requirements. Therefore, we extend traditional attribute-based access control to support this kind of security requirements which is common in practice.

A visibility policy is used to formalize the term of "who have also handled this product" in the above example. For two supply chain partners *A*, *B* and an EPC *e*, there is a relationship between *A* and *B*: they are either in the same supply chain of *e* or not. This kind of relationship can be used to specify access control policies as shown in Example 1. Because such access control policies are related to the visibility of supply chains, we call them visibility policies.

In this paper, we consider the following three kinds of visibility policies: whole-stream policy, up-stream policy and down-stream policy.

Definition 1. (whole-stream policy for EPC *e* defined by supply chain partner *scp*) The event information belonging to supply chain partner *scp* regarding EPC *e* can be accessed by any supply chain partners who have also handled the product associated with EPC *e*.

Definition 2. (up-stream policy for EPC *e* defined by supply chain partner *scp*) The event information belonging to supply chain partner *scp* regarding EPC *e* can be accessed by any supply chain partners who have also handled the product associated with EPC *e* before *scp* handles it.

Definition 3. (down-stream policy for EPC *e* defined by supply chain partner *scp*) The event information belonging to supply chain partner *scp* regarding EPC *e* can be accessed by any supply chain partners who have also handled the product associated with EPC *e* after *scp* handles it.

4.1. Extended attribute-based access control

Traditional attribute-based access control policies are specified based on subject attributes and object attributes. Our extended attribute-based access control policies involve an additional attribute: visibility attribute.

- Subject attributes: A subject is a user, who queries or operates on event information. Each subject is associated with a set of attributes which define the identity and characteristics of the subject. Subject attributes may include subject identifier, name, country, and etc.
- Object attributes: Object attributes are attributes of event, including EPC, Time, and etc.
- Visibility attributes: Visibility attributes take three values: whole-stream, up-stream, and down-stream.

An ABAC authorization language (AUL) is used to define who is allowed to perform what kind of query operations on what kind of data. The AUL is defined as follows:

AUL:= object-condition ∧ subject-condition
| object-condition ∧ visibility-condition
| object-condition ∧ subject-condition
∧ visibility-condition

where subject-condition, object-condition and visibility-condition are all Boolean conditions for subject attributes, object attributes and visibility attributes, respectively. All these conditions are constructed with the following rules:

Condition := expression | condition op condition
| (condition op condition)
Expression := attribute comp value |
Attribute comp attribute |
Attribute comp {value_set}
Op := and | or
Comp := < | > | <= | >= | = | [NOT] Like | [NOT] IN
Value_set := value | value, value_set

Example 2. Using the extended attribute-based access control policy language, the policies in Example 1 can be specified as follows:

- *P1 = Time > 2011-01-01 ∧ Visibility = whole-stream ∧ Role = distributor;*
- *P2 = EPC like urn:epc:id:404958810:* ∧ Visibility = down-stream;*
- *P3 = Time > 2011-03-01 ∧ Visibility = up-stream.*

The extended attribute-based access control is powerful in terms of expressiveness as it is more generic than traditional attribute-based access control. However, it is not easy to enforce it efficiently. We exploit two critical techniques to enforce extended attribute-based access control in practice: policy transformation and query modification.

Policy transformation is used to transform ABAC policies into fine-grained access control (FGAC) policies. In an FGAC policy, it assigns an SQL predicate to a user so as to express which data can be accessed by the user. FGAC policy is a special case

of ABAC policy where the attribute of a subject is a user's ID. The transformation of an ABAC policy into FGAC policies takes two steps. First, an ABAC policy can be used to derive three different conditions: subject condition, object condition and visibility condition with subject attributes, object attributes and visibility attributes, respectively. Second, all users, who satisfy the subject condition, are associated with the object condition and the visibility condition.

Query modification is used to enforce the transformed fine-grained access control policies. The basic idea of query modification is that before being processed, user queries are transparently modified to ensure that users can access only what they are authorized to access. The modification of a query takes in there steps. First, the visibility condition in FGAC policy is transformed into a SQL predicate. Then, the SQL predicate and the object condition are combined to construct a temporary view. Finally, the temporary view is used to replace the corresponding table in user's query. The detail of this process is provided in our previous paper [8].

4.2. Implementation of SecEPCIS and SecEPCDS

We implement SecEPCIS by extending Fosstrak EPCIS [20] to support attribute-based access control with the following components: policy management, policy service, policy transformation, policy storage, policy publish, data publish and policy interface. In SecEPCIS, access control policies can be created by supply chain partners to protect their data. These policies can be published into SecEPCDS automatically if such choice is made. Users' queries are checked and modified under the corresponding access control policies before being executed.

We implement our SecEPCDS prototype from scratch following the design introduced in Section 3.3. In SecEPCDS, supply chain partners can publish event index information from their EPCIS systems and users can submit query for EPCIS systems which store the detailed event information of interest. In order to protect the data in SecEPCDS, supply chain partners can define attribute-based access control policies which are enforced against users' queries. Our SecEPCDS is developed in C-Sharp using SQL SERVER 2005 as its database.

All interfaces in the secure platform of EPCglobal network are implemented as web services which are suitable for information sharing among distributed supply chain partners.

5. Discussion

In Section 1, we provide three primary goals to guide the design of the secure platform for EPCglobal network services: 1) facilitating global information sharing among supply chain partners; 2) supporting authorization mechanism; 3) reducing the cost of managing and maintaining supply chain partners' data and authorization policies. All of these goals are met in the proposed secure platform.

First, SecEPCDS is designed and implemented to facilitate global information sharing among supply chain partners. Each supply chain partner can publish index information into SecEPCDS through his own SecEPCIS. Users can locate SecEPCIS systems with the help of SecEPCDS and further query the corresponding SecEPCIS systems for detailed event data of interest. Users can also request SecEPCDS to help in querying the corresponding SecEPCIS systems and returning the aggregated result to them, since the aggregating model is supported in the platform. It is especially useful for those users who have limited computation and communication capabilities (e.g. mobile devices).

Second, the authorization mechanisms are designed and implemented in SecEPCDS and SecEPCIS respectively. Supply chain partners can specify access control policies in SecEPCDS and SecEPCIS to protect their data.

Third, in order to reduce the cost of managing data and access control policies, the data publish and policy publish mechanisms are designed and implemented in SecEPCIS. These two mechanisms help supply chain partners publish their event data and policies into SecEPCDS automatically.

6. Track & Trace Application

A track & trace application is one of the most important application in the EPCglobal network. In a track & trace application, supply chain partners can monitor their product in real time and optimize supply chain management; on the other hand, end consumers can evaluate the products they purchase. We design and implement a web-based track & trace application leveraging on EPCglobal network services. While supply chain partners can build their own track & trace applications leveraging on the interfaces provided in EPCIS and EPCDS, our track & trace application shows how this can be done in a large scale, including providing track & trace services to the end consumers. Our track & trace application, named DSIOT, is a web-based application which allows end consumers to tap on EPCglobal network from their desktop, laptop or even mobile phone.

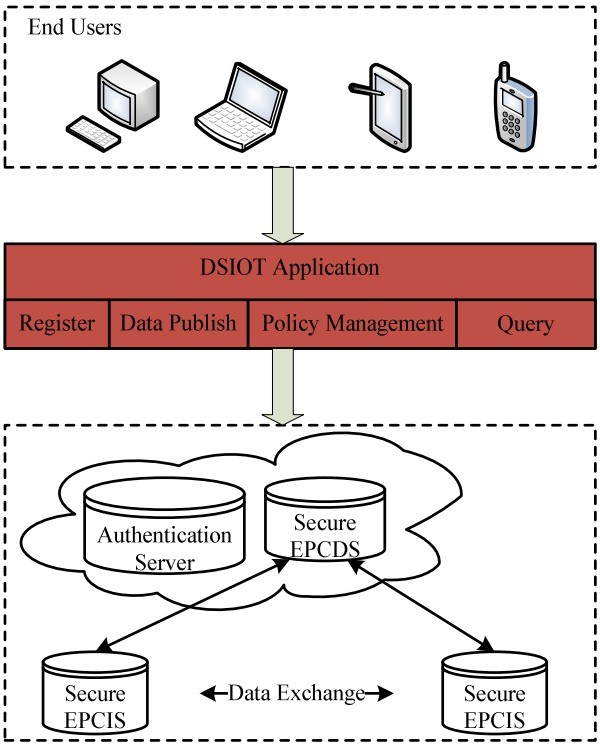

Figure 10. Architecture of DSIOT

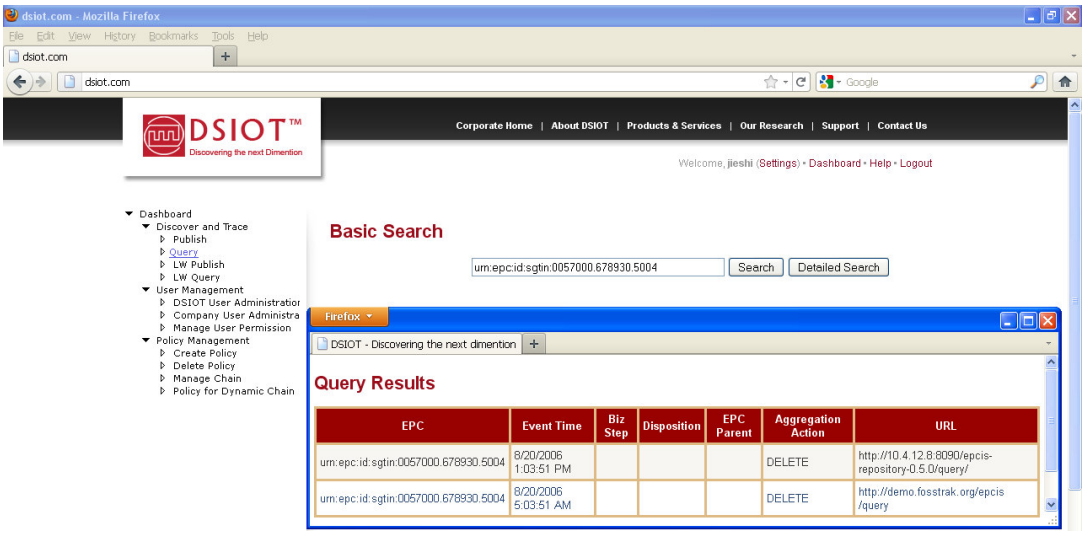

Figure 11. Screenshot of DSIOT for an abstract query

There are two goals for DSIOT application. First, it should allow supply chain partners and end consumers to easily track and trace products. Second, it should facilitate data management and policy management of supply chain partners. With DSIOT, supply chain partners can easily publish their data into EPCDS, mange their authorization policies and track products in supply chains. In particular, four kinds of functionalities are provided in DIOST:

- Register: Any supply chain partner or end consumer can register into EPCglobal network through DSIOT;
- Data publish: Supply chain partner can publish data into secure EPCDS system through DSIOT;
- Policy management: The security administrators of supply chain partners can define, modify and delete authorization policies in secure EPCDS system through DSIOT;

- Query: Any supply chain partner or end consumer can track & trace object in supply chain network by submitting queries to DSIOT.

The architecture of DSIOT is shown in Figure 10. DSIOT is a web application built on top of secure EPCglobal network services so that supply chain partner or end consumer can access it through web browser. The DSIOT application interacts with the authentication server and the secure EPCDS system to achieve its goal. When supply chain partners register into the EPCglobal network, DSIOT sends the information to authentication server to complete the task; when supply chain partners submit data into EPCDS system or query information from EPCDS system, DSIOT sends the data or query to EPCDS system and shows results to end users. Since secure EPCDS system supports three different models - directory model, relay model and aggregating model, DSIOT provides three types of query for end users, namely abstract query, relay query and aggregating query. By sending abstract query, end users would receive the addresses of corresponding EPCIS systems; and by sending relay query, end users would receive detailed event information from corresponding EPCIS systems; by sending aggregating query, end users would receive the aggregated event information from EPCDS system. Figure 11 shows a screenshot of DSIOT for an abstract query.

7. Conclusion

The EPCglobal network, as an industrial standard, provides a platform to share information among supply chain partners. In order to protect the valuable information in EPCglobal network, we design a secure platform for information sharing in EPCglobal network which supports authentication and authorization. We also show the feasibility of our design by implement it with a web-based secure track & trace application.

8. References

[1] J. Shi, Y. Li, R.H. Deng and K. Chiew. "Design and implementation of a secure prototype for EPCglobal network services". In RFIDSec Asia, pp. 45-56, 2012.

[2] B. Fabin and O. Günther. "Security Challenges of the epcglobal network". Commun. ACM, 52(7): 121-125, 2009.

[3] Y. Wu, D.C. Ranasinghe, Q.Z. Sheng, S. Zeadally, and J. Yu, "Rfid enabled traceability networks: a survey". Distributed and Parallel Databases, 29(5-6):397-443, 2011.

[4] EPCglobal architecture, http://www.epcglobalinc.org.

[5] J. Muller, J. Oberst, S. Wehrmeyer, J. Witt, A. Zeier, and H. Plattner. "An aggregating discovery service for the epcglobal network". In Proceedings of the 43rd Hawaii International Conference on System Science, pp. 1-9, 2010.

[6] A. Juels. "Rfid security and privacy: a research survey". IEEE Journal on Selected Areas in Communications, 24(2): 381-394, 2006.

[7] B. Liu and C.-H. Chu. "A fine-grained authentication method for inter-domain epcglobal network". In Workshop on RFID Security – RFIDSec Asia' 11, pp. 21-34, 2011.

[8] J. Shi, D. Sim, Y. Li, and R. Deng. "Secds: a secure epc discovery service system in epcglobal network". In CODASPY, pp. 267-274, 2012.

[9] B. Liu and C.-H. Chu. "Security analysis of EPC-enabled RFID network". In IEEE International Conference on RFID-Technology and Application, pp. 239-244, 2010.

[10] S. M. Kywe, J. Shi, Y. Li, R. Kailash. "Evaluation of different electronic product code discovery service model". In Advances in Internet of Things (AIT), 2(2): 37-46, 2012.

[11] S. Evdokimov, B. Fabian, S. Kunz, and N. Schoenemann. "Comparison of discovery service architectures for the internet of things". In SUTC, pp. 237-244, 2010.

[12] E. Grummt and M. Müller. "Fine-grained access control for epc information services". IOT, pp. 35-49, 2008.

[13] B. Fabian. "Implementing secure p2p-ons". In ICC, pp. 1-5, 2009.

[14] B. Fabian, T. Ermakova, and C. Müller. "SHARDIS: A privacy-enhanced discovery service for rfid-based product information". IEEE Transactions on Industrial Informatics, 2011.

[15] Q. Yan, Y. Li, and R.H. Deng. "Anti-Tracking in RFID discovery service for Dynamic supply chain systems". International Journal of RFID Security and Cryptography (IJRFIDSC), 1(1/2): 25-35, 2012.

[16] J. Shi, Y. Li, W. He, and D. Sim. "SecTTS: A secure track & trace system for RFID-enabled supply chains". Computers in Industry, 63(6): 574-585, 2012.

[17] GS1. RFID Security & Privacy Lounge. http://www.avoine.net/rfid/index.php, 2011.

[18] P. Samarati and S. De Capitani di Vimercati. Access control: Policies, model, and mechanism. In FOSAD, pp. 137-196, 2000.

[19] E. Yuan and J. Tong. Attribute-based access control (ABAC) for web services. IEEE International conference on web services, 0:561-569, 2005.

[20] Fosstrak. Fosstrak epc information services. http://code.google.com/p/fosstrak/wiki/EpcisMain

