<table>
<thead>
<tr>
<th>Title</th>
<th>Auto-ID enabled tracking and tracing data sharing over dynamic B2B and B2G relationships</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Xu, FJ; Tong, FCH; Tan, CJ</td>
</tr>
<tr>
<td>Issued Date</td>
<td>2011</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10722/176098">http://hdl.handle.net/10722/176098</a></td>
</tr>
<tr>
<td>Rights</td>
<td>Creative Commons: Attribution 3.0 Hong Kong License</td>
</tr>
</tbody>
</table>

Frank J. Xu, Frank C. H. Tong, Chung Jen Tan
E-Business Technology Institute
The University of Hong Kong
HKSAR, The People’s Republic of China
{fxu, ftong, ctan}@eti.hku.hk

Abstract—Growing complexity and uncertainty are still the key challenges enterprises are facing in managing and re-engineering their existing supply chains. To tackle these challenges, they are continuing innovating management practices and piloting emerging technologies for achieving supply chain visibility, agility, adaptability and security. Nowadays, subcontracting has already become a common practice in modern logistics industry through partnership establishment between the involved stakeholders for delivering consignments from a consignor to a consignee. Companies involved in international supply chain are piloting various supply chain security and integrity initiatives promoted by customs to establish trusted business-to-customs partnership for facilitating global trade and cutting out avoidable supply chain costs and delays due to governmental regulations compliance and unnecessary customs inspection. While existing Auto-ID enabled tracking and tracing solutions are promising for implementing these practices, they provide few efficient privacy protection mechanisms for stakeholders involved in the international supply chain to communicate logistics data over dynamic business-to-business and business-government relationships. A unified privacy protection mechanism is proposed in this work to fill in this gap.

Keywords: Tracking and tracing, Privacy protection, Data sharing, Auto-ID, Business-to-business, Business-to-government, Logistics and supply chain

I. INTRODUCTION

Supply chain management is becoming more complex and fragile today than before, due to globalization, economic crisis, thriving of emerging economies such as Brazil, Russia, India and China, increasing logistics cost, rapidly changing customer’s demand and consumption patterns, serious natural disaster, terrorism and politics turmoil. Supply chain management includes various activities, such as planning, sourcing, manufacturing, delivering, recycling, relationship building, contract negotiation, finance management, risk management, data management, business and government regulatory compliance. The international end-to-end supply chain is evolving from simple chain or structured network into complex, fluid/dynamic, global ecosystem, involving more and more enterprises, government units, service providers and people, technologies/systems and business models [37, 41].

Logistics and supply chain management is becoming even more challenging for retailers, manufacturers and logistics enterprises in Hong Kong and China. In Pearl-River-Delta region of China, there are about 100,000 manufacturers, of which about 57,500 are invested by Hong Kong. In the past, these enterprises created added-value only through simple processing operations, cheap and skilled labors for fulfilling requirements of export markets. Today, they are targeting both inland and outland markets through value chain extension, industry updates and transformation. The region has already become the major sources and destinations of global supply chain. The industries are facing unprecedented challenges and opportunities rising from rapid development of China’s logistics infrastructure, huge and diversified inland consumer markets, China’s close integration and competition with neighbors.

To tackle these challenges, enterprises are continuing innovating management practices and piloting emerging technologies for achieving supply chain visibility, agility, adaptability and security through business-to-business (B2B) relationship development and management with national, regional and international customers and stakeholders. For example, manufacturers and retailers are continuing outsourcing their logistics operations to freight forwarders or third party logistics (3PLs) providers. Freight forwarders usually organize logistics activities through subcontracting for delivering consignments from a consignor to a consignee, meaning that a prime logistics service provider subcontracts its contracted logistics service from the consignor to specialized companies to execute individual logistics operations, such as consolidation and deconsolidation, packaging, warehousing, cross-border ocean shipping, air, train and truck transportation [13, 38]. In China and Hong Kong, these practices are becoming more popular. Based on the report by China Association of Warehouses and Logistics, about one third of manufacturers and one fifth of retailers in China have already outsourced their logistics to 3PLs. For companies adopting 3PL, over 50% of them outsource their logistics to more than four companies [25]. Besides, China’s rapidly growing e-commerce market is generating more requirements for 3PL [19]. In the world, a few forward-looking companies are splintering their traditional holistic supply chains into smaller and agile ones and reconfiguring their manufacturing sites to fight against higher levels of complexity and uncertainty in the future [37].
Close business-to-government (B2G) relationships are persistently pursued by government agencies, especially customs, and the private sector to achieve in-transit visibility and reduce security threats, vulnerabilities and uncertainties associated with customs supervision and declaration along the international trade and supply chain. Main objectives of the Framework of Standards to Secure and Facilitate Global Trade (SAFE) endorsed by the World Customs Organization (WCO) are to secure, smoothen and facilitate global trade through partnership establishment between private and government involved in international trade supply chains [42]. Implementation of the SAFE Framework includes Authorized Economic Operator (AEO) initiatives launched by European Commission, Customs-Trade Partnership Against Terrorism (C-TPAT) Programme and Container Security Initiative/10+2 Importer Security Filing Initiative by the US, all of which aim to gain greater visibility into the cargo flow of global trade for improving supply chain security [16, 22, 28, 33, 34, 39, 40]. Up to 2010, there are over 30 different AEO programmes in 56 countries. In China, the General Administration of Customs has launched Classified Management of Enterprises Programme since April 2008, and 1,577 enterprises have already been certified as the AEOs (Class AA enterprise) by March 2010 [39]. The Hong Kong Customs has started the HK Authorized Economic Operator Pilot Programme since June 2010. The programme is customized to fit the unique local trading environment of Hong Kong, which is characterized by a significant proportion (about 98%) of small and medium enterprises, for further enhancing the efficiency and competitiveness of the Hong Kong logistics industry [24, 45].

Accurate, reliable, comprehensive and real-time cargo flow data is the key to achieve supply chain visibility and security through the establishment of trusted B2B relationship including subcontracting, and B2G partnership. Auto-ID technology and Internet of Things, such as barcode, Radio Frequency Identification (RFID), sensor network, global positioning systems (GPS), are promising enablers for collecting, processing and exchanging the data, allowing automatic identification and trajectory capture of moving cargos at item, pallet, consignment, container and vessel levels, and real-time distribution of the captured data to related parties [12, 20, 21, 23]. Though these technologies can greatly improve the visibility, security and efficiency of supply chain operations and government administration, they present involved parties with potential risks of disclosing sensitive and valuable business information to unauthorized invaders or business competitors. Dynamics and complexities of B2B relationship, including subcontracting, and B2G relationship make it even more difficult for the involved stakeholders to share tracking and tracing cargo flow data in efficient and secure ways with traditional role-based database administration model. A lightweight privacy protection mechanism has been proposed in our previous work, allowing these data accessing and operations over enterprise subcontracting relationships, but few B2G business requirements and contexts are considered [43]. To satisfy both needs of B2B (including subcontracting) and B2G business and facilitate the wider adoption of Auto-ID technologies for achieving supply chain visibility and security, unified and flexible data sharing policies and reliable security control mechanisms have to be developed.

As an extension to our previous work in [43], a unified privacy protection mechanism is proposed in this paper for the involved parties to register and cancel strategic and operational relationships, to set up and clear cargo shipment jobs information under predefined partnerships, and to update and clear tracking and tracing data relating to a specified job or partnerships.

The rest of the paper is organized as follows. In section II, problems are identified through scenario analysis and reviews on prior works relating to Auto-ID technology enabled tracking and tracing solutions, security and privacy control mechanisms for communicating and accessing tracking and tracing data. The unified privacy protection mechanism for data sharing over dynamic both B2B and B2G relationships is presented in Section III. Section IV introduces a method to implement the proposed mechanism when developing tracking and tracing public service platforms or port community systems. Future work and a short conclusion are given in the last section.

II. RELATED WORKS

A typical international supply chain scenario is shown in Fig. 1 for demonstrating the involved organizations, business activities, physical, information and financial flows between the organizations. There are three different but interrelated layers. The first layer relates to physical activities and physical flows, such as transport and transshipment. The second layer is a layer of contracting or transaction activities over all commercial B2B relationships between the involved parties. Most of the information relating to the commercial trade and logistics process originates from this layer. The third layer is a layer for governance and regulation compliance, in which all governing bodies like customs, inspection authorities, port polices, and their inspection and verification activities are included. The second and third layers consist of information and financial flows.

![Figure 1.Layered Model of International Supply Chain [38].](image)

Logistics operations in above scenario is initiated either by a shipper (consignor) who is the sender or receiver (consignee) of the goods to be packaged and delivered from origin country $A$ to destination country $B$. The organization of the logistics is typically done either by a carrier nominated directly by the shipper or receiver of the goods, or performed by a subcontractor of the carrier, e.g. the shipping line agent.
Nowadays, it has become more common that other organizations, such as logistics service providers, organize the logistics. The logistics service providers take responsibilities on the overall planning and control of (parts of) the supply chain, where operational responsibilities are outsourced to specific logistics operators in the physical layer. Organizing the transport of a container can be done in different ways. The shipping line may outsource the complete hinterland transport operation to a logistics service provider, where several transportation modes and inter-modal transshipment need to be coordinated. Besides, customs declaration and clearance agents, trading, finance and insurance service providers may be involved to fulfill the delivering order as well.

To enhance safety and security of international supply chain, government organizations, such as customs, port authorities, sea port and river polices, inspection and quarantine authorities, are usually involved to administer and monitor the cross-border movement of cargos. Logistics and supply chain companies are required submit paper documents or electronic information to these organizations for complying with national and international trading laws, import and export rules and regulations. Activities performed by these government organizations, originally aiming to enhance safety and security, could lead to supply chain disruptions. For example, imported cargos without complete and accurate customs declarations will be recognized as high-risk cargos. Once customs selects a container containing cargos for an X-ray scan and inspection, it will result in additional delays and costs.

In short-term multi-company network/alliance, the B2B relationship is created at the start of execution of a delivery job/a service project and terminated when the job is completed. The shipper/consignor usually signs an outsourcing contract with a third party logistics provider (a freight forwarder) for delivering goods to its customers (the consignee). The logistics third party logistics provider then subcontracts individual logistics jobs to specific logistics operators, e.g. local shipper and cargo liner operator. The local shipper can further subcontract its jobs to consolidator, barge operator and customs declaration and clearance agent. These jobs can be subcontracted again to truck carrier and consolidation centre operator by the consolidator. Depending on the varieties of logistics operations a delivery job demands, either hierarchical or networked business/subcontracting relationship is established between the involved logistics service provider and logistics operators. Multiple jobs could be completed under one single subcontracting relationship, or be fulfilled individually under different subcontracting agreements. Functions and issues of various tracking systems for multi-company environments are thoroughly studied in [23, 30]. To handle the tracking issues resulted from dynamic B2B relationships in short-term multi-company distribution networks, a novel forwarder-independent approach for tracking material flow is proposed; followed by prototype implementation, open source development, industrial pilots and concept evolution through project DIALOG, TraSer and PROMISE. Main contribution of the approach is the introduction of ID@URI tracking code concept which can be encoded and attached to moving items, pallets and containers for tracking and tracing the trajectory of individual object [12, 23, 30].

B2G relationships (Customs-to-Business) being promoted by various AEO programmes/initiatives in many countries, are still stay at strategic level. They need to be implemented through operational activities. To make better use of trusted B2G relationships and raise the AEO concept to new heights of private and government partnerships, customs experts advocate developing seamless electronic data ‘pipeline’ linking the consignor and the consignee across the whole international supply chain [20, 21]. They argue that real-time, accurate data must be assured from the beginning and the originator, updated when the goods move and are merged in transit and shared in a risk based layered approach. This will require harmonized data model, facility and reliable privacy protection mechanism for data interchange between B2B and B2G business transactions [40].

There are two levels of security control in deploying Auto-ID technologies in tracking and tracing applications: lower level in data communication and higher level for data sharing in the context of business relationship. In the following description, we just take RFID application as an example, which can be easily extended to other Auto-ID technology enabled applications. Lower level security control mainly focuses on the authentication of RFID reader and tag, encryption and decryption of the message transmitted between reader and tag, while higher level security control focuses on identity or role based data accessing and data sharing mechanisms, which are widely used in traditional database management applications [3, 4, 5, 14, 29, 32, 36].
For distributed RFID data management mechanism, a series of standards developed by industrial the consortium EPCglobal provide architectural and technical guidance on RFID data management, including data capturing, filtering, storage, accessing and sharing in global supply chain tracking and tracing applications [7, 8, 9]. These standards assume RFID data is collected at different sites and stored in a network of distributed databases when items and products move between different organizations. Tracking and tracing data accessing and sharing are implemented through standardized query interfaces provided by each database. Though the recently published specification describes how security functions, such as authentication, access control, validation, and privacy protection of individuals and corporations, will be distributed across many of the roles/interfaces operating within the EPCglobal network, security is still a major issue, not fully addressed in EPCglobal’s standards to handle the inherent complexities arising from B2B relationship (including subcontracting) and B2G partnership in the international supply chain tracking and tracing [1, 2, 5, 10, 27, 35].

By leveraging EPCglobal standards, an integrated security control mechanism is introduced in [17, 18] to handle the privacy protection and security issues in dynamic supply chain tracking and tracing applications. The mechanism comprises a tag-reader security scheme, and proposes a higher level Circle-of-Trust model (COT) for sharing tracking and tracing data. Though this mechanism is a promising solution, it is too generic and its implementation needs great efforts to efficiently describe complex relationships between logistics enterprises (e.g. semantic technologies could be used). The mechanism does not consider the requirements of B2G business either. In addition, a distributed network like EPCglobal network has to be established to apply this mechanism. For logistics enterprises with complex and dynamic subcontracting business relationships, especially for those not joining in the network or having great security concerns to link the network, an easy-to- implement solution is still in urgent need for our studying cases.

A generic traceability data model and an innovative combination of query processing method and data sharing techniques borrowed from peer-to-peer networks, distributed and parallel databases are presented in [1]. The model and the techniques enhance the security of tracking and tracing data sharing throughout logistics and supply chain management in the sense that: 1) each involved stakeholder is given complete sovereignty over its own data including business relationships information; 2) incoming query is executed and rewritten based upon pre-designed data sharing policies, which can be installed and modified without interaction with other parties. This mechanism still relies on database accessing control and privacy protection mechanism in the sense that each participant within the traceability networks is required to exactly define and enforce which data will be disclosed to which query, which is not easy to adopt and implement for the enterprises and government agencies with dynamic B2B, B2G relationships in the international supply chain.

Another access control model is proposed for monitoring mobile physical objects in logistics and supply chain management, which allows users to implement security control and data sharing measures based on pre-set trajectory visibility policies [31]. Being well-suited for distributed RFID systems, this model is an extension to attribute-based access control model, which originally aims to enable dynamic and fine-grained data sharing in service oriented environment [44].

For central RFID data management solution, an RFID cube is introduced to support warehousing and analysis of massive RFID data sets in [15]. Oracle presents a new bitmap data type for Oracle DBMS to support RFID-based item tracking applications [26]. Both solutions assume that RFID data is collected and updated from separate users, and is stored within a single data repository. To tackle the efficiency issues arising from incremental real-time RFID data update and analytical ad-hoc querying of central RFID data management solution, a single database approach is introduced, which merges OLAP (On-Line Analysis Processing) and OLTP (On-line Transaction Processing) components in only one central database system [6]. Security and confidentiality of RFID data are not fully addressed in all of these central management solutions once it is collected and uploaded into the central data repository.

Establishment of trusted B2B and B2G relationships and adoption of state-of-the-art Auto-ID tracking and tracing solutions in international supply chain management are both for achieving supply chain visibility and security. Without flexible and reliable privacy protection mechanism for integrating the two, the supply chain will become ‘only as strong as its weakest link’. In the prior works described above, most solutions focus on pre-set data accessing rules/policies except the one in [17, 18], which can not efficiently handle the dynamics of B2B and B2G relationships. In addition, as far as we know, few works have been done in unifying the privacy protection mechanism for communicating tracking and tracing data over dynamic B2B relationship including subcontracting and B2G relationship.


To fill in the gap in Auto-ID enabled logistics tracking and tracing data sharing over dynamic B2B and B2G relationships, we extend our work in [43], and propose a unified privacy protection mechanism in this paper. The mechanism consists of a set of protocols for the involved stakeholders in international supply chain to register and cancel strategic and operational partnerships, to set up and clear logistics jobs in accordance with dynamic partnership engagement, to update and clear cargo flow data captured with Auto-ID technology relating to a specified job or partnership, to query subcontracted job execution progress and history, to fulfill compliance requirements of government and trade regulations, and to identify potential threats and risks in real-time.

Fig. 3 illustrates use cases corresponding to each protocol of the proposed mechanism: A) prime enterprise registers B2G relationship with government organizations (including customs and border enforcement agencies) based on its AEO status; B) prime enterprise registers B2B relationship (e.g. subcontracting) with its business partners/ subcontractors; C) prime enterprise sets up task information to be outsourced to its subcontractors; D) prime enterprise queries the execution progress of specified
logistics job; E) prime enterprise submits real-time cargos flow data to customs for customs declaration and pre-arrival risk analysis; F) prime enterprise clears outsourced job’s information; G) prime enterprise de-registers contracting relationships with subcontractors; H) prime enterprise updates/terminations its relationships with government organizations; I) subcontractors scan moving logistics objects, equipments, items and products with RFID tags or sensors attached and upload encrypted monitoring data; J) customs and border enforcement agencies inquire detailed description and traceability information on high-risk cargos; K) public users query the traceability information of the products they consume; Here, the prime enterprise refers to the company who is responsible for organizing and coordinating the overall cross-border logistics and supply chain management operations. Due to the complexities in existing transport and logistics procedures, freight forwarder usually takes the role on behalf of the consignor or consignee, especially for small and medium sized enterprises.

Fig. 4 and Fig. 5 describes the protocols of the proposed mechanism in simplified data flow diagrams, depicting message flows between prime enterprise, its subcontractor, government organization/customs, prime enterprise’s application system, subcontractor’s application system, customs’ system, data capturing system with Auto-ID devices, and B2B, B2G relationship based tracking and tracing service platform. The B2B, B2G relationship based tracking and tracing service platform could be a sub-system in some country’s Single Window platforms or some port community service platforms.

Denoting the prime service enterprise as data owner O, its subcontractor as C, government organization as G, jobs outsourced by O to C as J, items identification related to J as ID, location where Auto-ID devices are deployed as L, tracking and tracing controlling points as X, tracking and tracing service platform as P, data capturing system with Auto-ID devices installed at location L as E, government organizations as G, government supervision system as S, the message flows can be described as the following:

1) The prime enterprise needs to initialize and set up job information for outsourcing it to subcontractors (solid lines in Fig. 4) and submitting required data for trade and government regulations compliance (e.g. customs manifests and way bills). The job information includes the job related item and product IDs, Auto-ID devices locations, tracking and tracing control points etc. First, O sends job and control points’ information to P, job and control points’ information and item IDs to data capturing system E at Location L. Then, P stores job and control points information into its central data repository.

2) As shown in Fig. 4 in dotted lines, to register B2B relationship with a subcontractor to complete a specified job, the prime enterprise needs to send to P its own identity information, its subcontractor’s identity information, and the subcontracted job-item ID pairs. P stores the information into its static data repository and notifies the subcontractor C to set up job.

![Figure 4. Message flows relating to use cases B, C, D, G, F, I, K in figure 3.](image-url)

3) Data capturing system E can upload captured data into P over secure communication protocols (see dashed lines in Fig. 4). When items and products pass through C’s logistics site L, C scans tags attached on these objects to get ID and logistics information written into the tags with fixed or handheld Auto-ID readers. Then, E digitally signs and encrypts the captured data, and sends the signed and encrypted data to P. In the end, P decrypts and verifies the data it receives, and stores the decrypted data into its dynamic data repository.

4) The prime enterprise and its subcontractors can track the outsourced job’s execution progress or trace back its execution history by enquiring P with user identity information and job identity information (see dash-dotted lines in Fig. 4). P will return the query results in standard report formats.

5) Public users can obtain traceability report of specified items and products by querying P with identification code, such as Electronic Product Code (see long dashed lines in Fig. 4). P will return the query results in standard report formats.

6) The prime enterprise can request the tracking and tracing service platform P to clear a specified job data by sending to P its user identity information and the information of the job to be cleared (see long dash-dotted lines in Fig. 4). Upon receiving clearing request, P will delete the dynamic data related to the job from its repository and notify C to clear the related job data. C will notify data capturing system E to delete the related job-item ID pairs.
7) As illustrated in Fig. 4 in long-dash-dot-dotted lines, to de-register subcontracting relationship with its subcontractor, the prime enterprise needs to request $P$ to delete the related job-contractor pairs by providing $P$ with its identity information and the specified job information. Besides, $P$ needs to update job location and control point information, and to notify $C$ to delete the related job information, and $E$ needs to delete the related job-item ID pairs.

8) To register B2G relationship with a government organization/customs, the prime enterprise needs to send to $P$ its AEO status information, its agreements with customs on the data requirements for customs declaration and clearance, and store the information into $P$’s static data repository (solid lines in Fig. 5). In some countries, business information with partners is required for certifying its whole supply chain passing, which can be retrieved from the prime enterprise’s application system by $P$.

9) The prime enterprise requests $P$ to submit the aggregated cargos flow data to government supervision organizations for customs declaration and clearance associated with the physical movement of the cargos in parallel, in advance or behind the cargos arrival (see dotted lines in Fig. 5).

10) Government supervision organizations (e.g. customs and inspection authorities) inquire detailed traceability information of high-risk cargos by querying $P$ with identification code of individual object, order or job ID on demand (see dashed lines in Fig. 5).

11) The prime enterprise requests $P$ to update B2G relationship when its AEO status or its agreements with government organizations changes (see dash-dotted lines in Fig. 4).

IV. AN IMPLEMENTATION METHOD OF THE UNIFIED PRIVACY PROTECTION MECHANISM

Major steps on how to implement the proposed mechanism include: 1) prime enterprise registers its partnership with government organizations based on its Class type (AEO status) certified by customs; 2) prime enterprise sets up outsourced job information; 3) once the information have been initialized and stored successfully in the static repository of the logistics tracking and tracing platform/system, the prime enterprise registers its business/subcontracting relationship with its subcontractors; 4) subcontractors start scanning objects passing through their sites and upload captured event data into the central dynamic data repository; 5) in the mean time, the prime enterprise, customs and border enforcement agencies, subcontractors and public users can query the execution progress of the outsourced job or trace the logistics history of a specified product/item; 6) to terminate business/subcontracting relationship with its subcontractors, the prime enterprise needs to de-register contracting information in the tracking and tracing platform; 7) after the outsourced job is completed, the prime enterprise can clear the job data stored in the logistics tracking and tracing platform and its own enterprise applications; 8) prime enterprise can update or terminate its tracking and tracing data in secure way. At the source point or consignment completion point of goods to be delivered, e.g. factory or exporter’s warehouse, RFID tags, sensor or bar code carrying product code information (e.g. Electronic Product Code) are attached to individual items, product boxes, or logistics equipments, e.g. pallets and containers. When the goods are in transit or pass through each logistics operation site equipped with Auto-ID enabled readers, their location information are recorded by scanning the attached tags or barcodes, and their ambient information (e.g. humidity and temperature) are captured by the deployed sensors. Auto-ID enabled readers include, but not limited to, RFID reader,
barcode reader and sensor, etc. Business information related to the item and product being scanned may need to be stored in and retrieved from enterprise applications. Various types of edge device middleware may be utilized for managing the Auto-ID devices, transforming the raw tag reads into meaningful events and business object data, signing and encrypting the data, and uploading the encrypted data into central tracking and tracing data repository through internet or virtual private network.

Core components of the B2B and B2G relationship based tracking and tracing prototype comprises of relationship management database, tracking and tracing management database, privacy management engine, tracking and tracing data processing engine. Relationship management database is a static repository for storing identity information of the prime logistics enterprise and its subcontractors, the prime enterprise’s AEO status information, business contract documents and data accessing rules for depicting B2B and B2G relationships. Tracking and tracing management database is a central dynamic repository for storing Auto-ID data submitted by subcontractors. Privacy management engine is responsible for identity verification of users requesting for data accessing and manipulation. Tracking and tracing data processing engine is responsible for parsing of user queries, dispatching of inquiry script commands to database, and formatting of returned query results.

The topmost level web-based user interfaces and web service interfaces of the prototype system provides different involved stakeholders with such privacy control and data sharing functions as: user administration, B2B and B2G relationship registration and de-registration, logistics control points set-up and cancellation, traceability query and tracking report generation.

V. CONCLUSION AND FUTURE WORK

Supply chain visibility and security are top objectives both enterprise and government supervision organizations are pursuing to achieve in managing and monitoring international trade and supply chain. Close B2B and B2G relationships and Auto-ID technology enabled solutions can facilitate realization of the two fundamentally contracting objectives, but need great supports of flexible and reliable privacy control mechanism for communicating tracking and tracing data between the involved stakeholders. Both role-based data accessing and sharing mechanism used in traditional database management applications and security control solutions based on EPCglobal infrastructure are not able to efficiently handle these issues together. In this paper, we proposes a unified privacy protection mechanism for the prime enterprise within a multi-company network, its business partners, and government organizations to share logistics tracking and tracing data captured with Auto-ID technology enabled systems. The mechanism consists of a set of protocols for the involved parties to register and cancel strategic and operational partnerships, to set up and clear logistics jobs to set up and clear logistics jobs in accordance with dynamic partnership engagement, and to update and clear tracking and tracing data relating to a specified job or partnership. A method for implementing the proposed mechanism in tracking and tracking service platform or port community systems is also introduced, including major use cases, data flows, and a high-level architecture of a prototype system.

The proposed mechanism and implementation method are motivated by direct requirements of several pilot enterprises in carrying out our R&D projects supported by the Innovation and Technology Fund. In the future, we will continue to follow up the progress of AEO programmes launched by the Hong Kong Customs, the China Customs and their counterparts in other countries. Feedbacks and new requirements (e.g. mutual recognition of AEO status between customs) from enterprises and related government supervision organizations will be consolidated to implement the proposed prototype through real logistics scenarios, such as tracking and tracing of Chinese medicine imported into Hong Kong from mainland China, transshipments and domestic sales of products manufactured by fully bonded and semi-bonded companies in China to verify the validity and efficiency of the proposed mechanism and implementation method.

ACKNOWLEDGMENT

This work is supported by the Innovation and Technology Fund (ITF) administered by the Innovation and Technology Commission of The Government of Hong Kong Special Administrative Region under the Innovation and Technology Support Programme, project ITP/018/09LP.

REFERENCES


