EPCglobal Network 상에서 EPC IS 와 EPCIS Discovery System의 연동을 통한 물류 정보 접근 제어 방법

문홍구° 한기덕 권혁철
부산대학교 컴퓨터 공학과
mhg09°@pusan.ac.kr, templer@pusan.ac.kr, hckwon@pusan.ac.kr

Method for Logistics Information Access Control on EPCglobal Network through the Interaction between EPC IS and EPCIS Discovery System

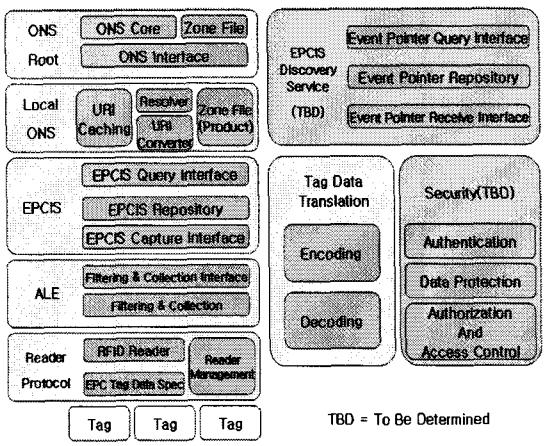
Honggoo Moon° Gideok Han Hyukchul Kwon
Department of Computer Science and Engineering, Pusan National University, Korea

요 약

본 논문에서는 EPCglobal Network 상의 물류 정보 시스템인 EPC IS(Electronic Product Code Information Services)와 EPCIS Discovery System의 기능을 확장하여 사용자 정보를 유지할 수 있도록 한다. 본 논문에서 EPC IS에 저장된 정보는 공개(Public)정보와 비공개(Private)정보로 나뉘고, 물류 정보 사용자에 따라 접근 가능한 정보가 다르다는 전제하에 물류 정보 사용자가 물류 정보 접근 시 사용자 정보를 유지하는 EPCIS Discovery System과 EPC IS의 연동을 통한 물류 정보 접근 제어가 이루어질 수 있도록 방법과 절차를 제안한다.

1. 서 론

EPCglobal Network는 EPC 코드와 RFID 기술을 근간으로 물류 정보 교환을 위해서 물류 객체에 EPC(Electronic Product Code)를 할당하는 방법에 대한 표준을 제공한다. 이를 통해 기업은 공급사슬(Supply Chain) 상에서 객체의 가시성, 추적성, 자동화, 보안성을 강화할 수 있게 되어 재고 최소화, 상품 손실 최소화, 주문의 신속한 처리, 소비자 기호 변화에 따른 대응능력 향상 등의 효과를 거둘 수 있다. 이런 EPCglobal Network는 RFID 태그 정보의 구조, 의미, 전달방법에 대한 표준은 제공하고, 개별기업은 EPCglobal Network 상에서 발생하는 정보를 각 기업과 기관의 방화벽 안에서 개별적으로 관리하고, 이 정보는 ONS(Object Naming Service)와 Discovery Service를 통해 공유하는 방식으로 운영된다. 이렇게 EPCglobal Network는 거대한 물류 환경에서 EPC정보의 분산관리와 전달 효율성을 높일 수 있다. 다음은 EPCglobal Network Architecture Framework를 보여주는 그림이다[1].



< 그림 1 EPCglobal Architecture Framework >

<그림 1> 에서 보듯이 EPCglobal Network Architecture는 EPC가 기록된 Tag, Tag의 정보를 읽어들이는 장치인 리더, 리더로 읽은 Tag 정보를 정제하고 취합, 중복된 정보에 대해서 제거와 정보의 그룹화 등의 역할을 하는 ALE, 정제된 EPC정보를 저장하고 제공하는

이 논문은 2007년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임 (지방연구중심대학육성사업/차세대물류 IT 기술연구사업단)

구실을 하는 EPC IS, EPCglobal Network 상에서 글로벌 검색서비스를 제공하는 ONS, EPCglobal Network에서 물류 정보사용자가 EPC에 대한 정보를 찾고 이에 접근할 수 있도록 하는 역할을 하는 EPCIS Discovery System으로 구성되어 있다. 현재 EPCIS Discovery System은 개념 단계의 논의만 되고 있으며, 그 외 물류 정보의 Security를 담당하는 부분 또한 아직 개념 단계의 논의만 되고 있다[2].

따라서 본 연구는 이러한 EPCglobal Architecture Framework를 기본으로 현재 개념 단계의 논의로만 진행중인 물류 정보의 접근 제어를 EPCIS Discovery System과 EPC IS의 사용자 정보 연동을 통해 효율적인 물류 정보 접근 제어 방법과 그 절차를 제시하는데 연구의 목적이 있다.

2. 관련연구

2.1 접근제어 모델

접근제어(access control) 분야는 컴퓨터 보안의 한 분야로서 꾸준히 발전해 왔다. 대표적인 접근제어 모델로는 강제적 접근제어(Mandatory Access Control)와 자율적 접근제어(Discretionary Access Control), 역할기반 접근제어(Role-Based Access Control), 과업-역할기반 접근제어(T-RBAC) 모델이 있다. 각각의 모델의 특징은 다음과 같다[3].

• 강제적 접근제어(Mandatory Access Control) : 각 정보에 결합한 비밀등급(classification level)과 사용자에게 부여된 인가등급(clearance level)을 사전에 규정된 규칙과 비교하여 그 규칙을 만족하는 사용자에게만 접근권한을 부여하는 보안정책으로서, 군사적 환경과 같이 정보의 기밀성이 매우 중요시되는 환경에서 사용되고 있다.

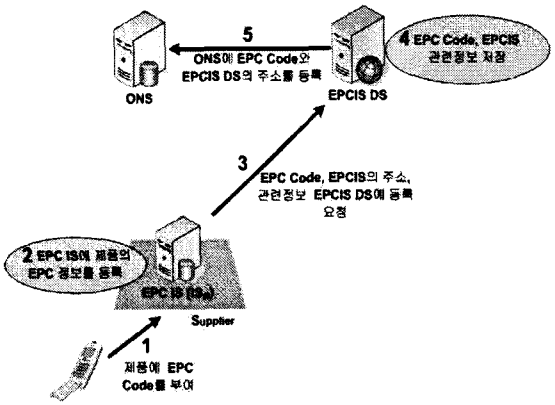
• 자율적 접근제어(Discretionary Access Control) : 정보객체의 소유자 혹은 관리자가 보안관리자의 개입 없이 자율적 판단에 따라 접근권한을 다른 사용자에게 부여하는 기법으로서, 정보보호보다는 정보의 공동 활용이 더 중요시되는 환경에 적합하다.

• 역할기반 접근제어(Role-Based Access Control) : 중심적인 개념은 정보 사용자가 기업이나 조직의 정보 자원에 마음대로 접근할 수 없도록 하는 것이다. 대신에 접근 권한이 역할(role)에 부여되고 사용자는 적절한 역할에 소속됨으로써 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 한다. 이러한 아이디어는 권한 관리를 매우 단순화시켜주고 기업의 특정한 보안정책을 구현하는 데 있어서 유연성을 제공하는 장점이 있다.

• 과업-역할기반 접근제어(T-RBAC)모델 : T-RBAC 모델에서는 정보객체에 대한 접근권한(permission)이 이를 요구하는 과업(task)들에 할당이 되고 이러한 과업들은 적절한 역할(role)에 할당된다. 사용자는 자신의 직위 또는 업무 역할에 따라 필요한 역할(role)들에 할당된다. 역할기반 접근제어(Role-Based Access Control)에 과업(task)의 개념이 추가된 접근제어 모델이다.

3. EPCglobal Networks 상에서의 정보 접근 제어

현재 개념 단계의 논의 중인 EPCglobal Network 상에서의 물류 정보 Security(물류 정보 접근 제어)를 지원하고자 종래의 EPCglobal Network에서 단순한 EPC관련 정보 저장, 제공 기능을 수행하던 EPCIS Discovery System과 EPC IS의 기능을 확장하여 사용자 정보 유지관리와 연동을 지원함으로써 효율적인 물류 정보 접근 제어를 위한 방법과 그 절차를 제안한다.



< 그림 2 EPC 등록 시나리오 >

<그림 2> 는 제품에 EPC Code가 부여되는 시점에 정보의 등록 시나리오를 보여주는 그림이다.
상품이 제조되면 해당 상품에 EPC Code가 부여되고, EPC IS에 EPC Code와 해당 상품정보를 저장한다. 그리고 EPCIS Discovery System에게 EPC Code와 EPC IS의 주소, 관련정보를 EPCIS Discovery System에 등록을 요청한다. EPCIS Discovery System은 등록요청한 정보를 저장한 후에 ONS에게 EPC Code와 EPCIS Discovery System의 주소등록을 요청하고 ONS는 이 요청을 받아서 처리한다.

< 표 1 EPC IS의 EPC 저장 정보 >

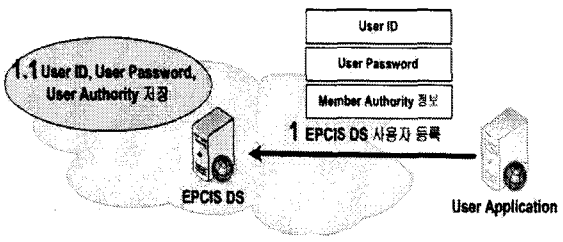
EPC IS 저장정보			
EPC Code1	제품정보 (Private)	제품정보 (Public)	Member Authority
EPC Code2	제품정보 (Private)	제품정보 (Public)	Member Authority
EPC Code3	제품정보 (Private)	제품정보 (Public)	Member Authority

<표 1> 은 EPC IS에 저장되는 EPC Code와 EPC Code에 대한 제품정보(Private, Public)와 EPC IS에 대한 Member Authority 정보를 보여준다. 저장되는 제품정보는 일반 사용자에게 모두 공개되는 Public 정보와 Member Authority를 가지는 사용자에게만 공개되는 Private 정보로 구분된다. Member Authority 정보는 일련의 권한으로서 EPC IS에 저장된 물류 정보 중 비공개 정보까지 접근할 수 있는 권한을 나타낸다. 여기서 Member Authority 정보는 EPC IS를 소유 관리하는 단체의 구성원들에게 사전에 제공되는 정보이다. 그리고 Member Authority 정보의 관리와 생성에 관한 것은 해당 EPC IS를 소유 관리하는 단체의 내부시스템의 역할이라는 것을 전제로 한다. 단지 EPC IS는 이렇게 관리된 Member Authority 정보를 저장하고 EPCIS Discovery System에 등록을 하면 되는 것이다.

< 표 2 EPCIS Discovery System의 EPC 관련 정보 >

EPCIS DS에서의 EPC 관련 정보		
EPC Code 1	URL Of EPCIS 1	Member Authority
	URL Of EPCIS 2	Member Authority
	URL Of EPCIS 3	Member Authority
EPC Code 2	URL Of EPCIS 1	Member Authority
	URL Of EPCIS 2	Member Authority
	URL Of EPCIS 3	Member Authority
EPC Code 3	URL Of EPCIS 1	Member Authority
	URL Of EPCIS 2	Member Authority
	URL Of EPCIS 3	Member Authority

<표 2> 는 EPCIS Discovery System에 저장되는 EPC 관련 정보를 보여준다. EPCIS Discovery System에서는 EPC IS에서 등록 요청을 한 EPC Code와 EPC IS 주소, 그리고 해당 EPC IS의 Member Authority를 저장하게 된다. 추후에 특정 EPC Code에 대한 해당 물류 데이터를 얻기 위해 EPCIS Discovery System에 접근하게 되면 EPCIS Discovery System는 접근한 사용자의 Member Authority와 EPC IS의 Member Authority를 비교하여 그에 합당한 Ephemeral Key(임시 키)와 EPC IS의 URL 목록을 사용자에게 제공한다.



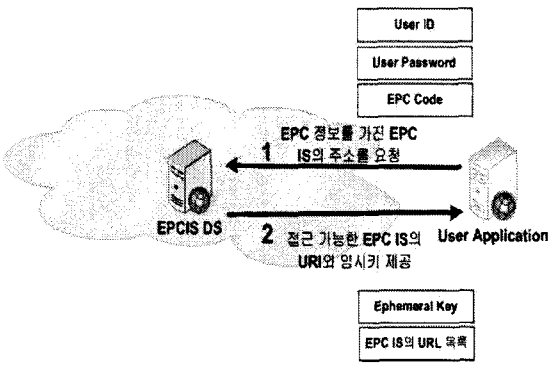
< 그림 3 EPCIS Discovery System 사용자 등록 시나리오 >

<그림 3> 은 EPCIS Discovery System에 사용자 등록 절차를 보여주는 그림이다. 사용자 응용프로그램은 EPCIS DS에 "User ID", "User Password", "Member Authority 정보"를 제공하고 EPCIS Discovery System은 사용자 정보를 저장함으로써 추후 사용자의 물류 정보 접근을 시도 시 적절한 물류 정보 접근 제어를 수행하게 된다.

< 표 3 EPCIS Discovery System의 사용자 정보 >

EPCIS DS에서의 사용자 등록 정보	
User ID	String
User Password	String
Member Authority	String

<표 3> 은 EPCIS Discovery System에 저장되는 사용자 정보를 보여준다. 먼저 User ID와 User Password가 저장되며, Member Authority라는 정보를 저장하게 된다. 여기서 Member Authority는 사용자가 특정 EPC IS를 소유한 단체의 일원임을 증명하며, EPC IS에 저장된 특정 EPC Code에 대한 Private(비공개) 정보에 접근 가능한 사용자임을 증명하는 정보이다. 추후 Member Authority를 가지는 사용자가 EPCIS Discovery System에 접근하여 특정 EPC Code에 대한 EPC IS 주소와 접근에 필요한 Ephemeral Key(임시 키)를 받을 때 사용자의 Member Authority에 맞는 Ephemeral Key(임시 키)를 받는다.



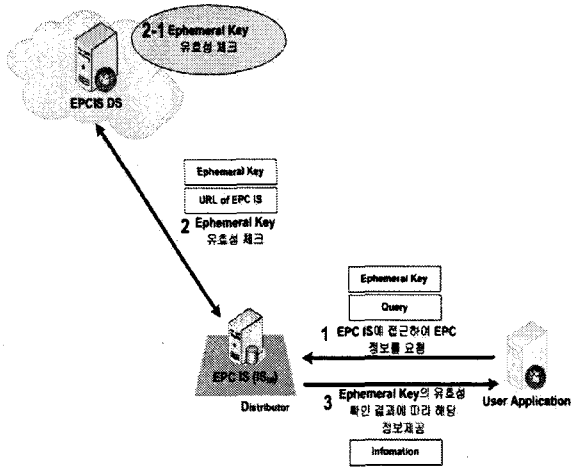
< 그림 4 사용자의 EPCIS Discovery System 접근 시나리오 >

<그림 4> 는 물류정보 사용자의 EPCIS Discovery System 접근 시나리오를 보여주는 그림이다. 사용자는 EPCIS Discovery System에 사용자의 "User ID", "User Password"와 함께 사용자가 얻고자 하는 정보의 "EPC Code"를 보내게 된다. 그럼 EPCIS Discovery System은 등록된 사용자의 정보를 검토(Member Authority 검토)하여 EPC IS의 URL 목록과 EPC IS 접근 시 이용되는 Ephemeral Key(임시 키)를 사용자에 제공하게 된다.

Ephemeral Key	
Access Authority	Member Authority

< 그림 5 Ephemeral Key의 구조 >

<그림 5> 는 Ephemeral Key(임시 키)의 구조이다. Ephemeral Key는 "Access Authority", "Member Authority"로 구성된다. "Access Authority"는 사용자가 EPC IS에 접근 시 EPC IS 접근의 권한을 나타내며, "Member Authority"는 사용자의 EPC IS를 소유하거나 관리하는 단체의 구성원임을 나타내는 권한이다. 만약 구성원이 아닌 일반적인 사용자일 경우 "Member Authority"는 일련의 기본 값으로 정해지게 된다.

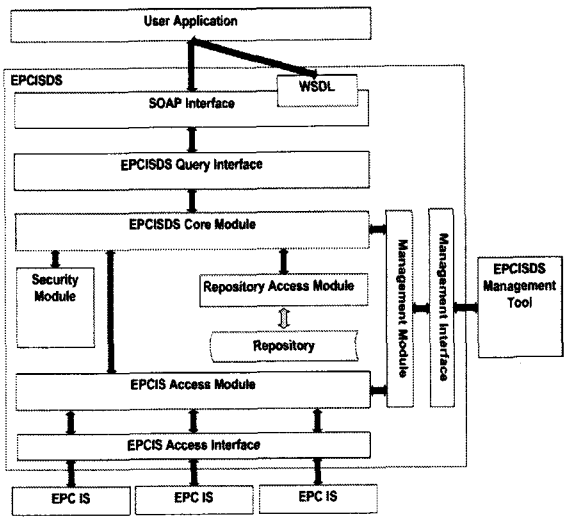


< 그림 6 사용자의 EPC IS 접근 시나리오 >

<그림 6> 은 물류정보 사용자의 EPC IS 접근 시나리오를 보여주는 그림이다. 사용자는 EPC IS에 접근하여 EPC 정보를 요청한다. 사용자가 EPC IS에 제공하는 정보는 "Ephemeral Key", "Query"이다. "Ephemeral Key"는 사용자가 EPCIS Discovery System으로부터 발급받아 EPC IS에 접근하기 위해 사용된다. 이 Ephemeral Key에 따라 해당 EPC IS의 접근 가능한 정보가 결정된다. 사용자로부터 정보제공의 요청을 받은 EPC IS는 사용자로부터 받은 Ephemeral Key의 유효성 검증을 하게 된다. 이때 EPC IS는 자신의 URL과 Ephemeral Key를 EPCIS Discovery System에 통보함으로써 Ephemeral Key의 유효성을 검증받게 된다. 유효성이 검증된 Ephemeral Key로 판명되었을 때 EPC IS는 사용자의 요구에 맞는 물류 정보를 제공하게 된다.

4. EPCIS Discovery System의 설계

다음 <그림 7> 은 분산 저장된 물류 정보에 대한 정보 접근 제어를 수행하는 EPCIS Discovery System의 설계도이다.



< 그림 7 EPCIS Discovery System의 설계도 >

User Application은 EPCIS Discovery System에 접근하여 정보를 획득하려는 사용자 응용프로그램이다. WSDL은 EPCIS Discovery System이 제공하는 웹서비스 기능들을 정의해 놓은 문서이다. 사용자 응용프로그램은 이 문서를 해석하여 EPCIS Discovery System에서 제공하는 기능들을 호출하는 방법을 알게 된다. SOAP Interface는 웹 서비스를 위한 통신 프로토콜 모듈이다. EPCISDS Query Interface는 SOAP Interface로부터 넘겨받은 Query를 분석하는 모듈이다. EPCISDS Core Moduled은 EPCIS Discovery System의 다른 모듈로부터 필요한 정보를 얻고 다른 모듈의 기능을 호출하는 등의 동작을 수행하여 EPCIS Discovery System이 제공하는 기능을 처리하는 코어 모듈이다. Security Module은 EPCIS Discovery System에서 유지하고 있는 사용자 Member Authority 정보와 EPC IS Member Authority 정보를 비교하여 물류 정보 접근 제어와 관련된 처리를 수행하는 모듈이다. Repository Access Module은 정보 저장소에 접근하기 위한 기능을 처리하는 모듈이며, Repository는 EPC Discovery System의 정보 저장소이다. Management Module은 EPCIS Discovery System 관리를 위해 필요한 기능들을 제공하는 모듈이며, Management Interface는 EPCIS Discovery System의 관리와 관련된 기능을 외부에서 호출할 수 있도록 제공하는 Interface이다. EPCISDS Management Tool은 EPCIS Discovery System의 관리 프로그램이다. EPCIS Access Module은 EPCIS Discovery System이 EPC IS와의 연동과 관련된 동작을 처리하는 모듈이며, EPCIS Access Interface는 EPC IS가 EPCIS Discovery System에 접근할 때 사용하는 Interface이다.

5. 결론 및 향후 과제

EPCglobal Architecture Framework를 기본으로 현재

개념 단계의 논의로만 진행 중인 물류 정보의 접근 제어를 EPCIS Discovery System과 EPC IS의 사용자 정보 연동을 통해 효율적인 물류 정보 접근 제어 방법과 그 절차를 제시하였다. 종래의 EPC IS의 EPC관련 정보 저장 기능을 확장하여 Member Authority 정보를 저장하였다. 물론 Member Authority 정보의 생성과 관리는 EPC IS를 소유 관리하는 단체의 내부시스템이 담당한다. 즉 EPC IS는 단순히 EPC 관련 정보에 Member Authority 정보를 추가 저장하고, EPCIS Discovery System에 등록함으로써 사용자 정보 유지 기능을 추가한 EPCIS Discovery System과의 연동을 통해 물류 정보 사용자의 물류 정보 접근 제어를 수행할 수 있다. 향후 연구 과제로 본 논문에서 제안한 물류 정보 접근 제어 방법을 적용한 물류 정보 시스템을 구현하고자 한다.

6. 참고문헌

[1] 리테일테크 기술연구소. "RFID 활용을 위한 네트워크 기술 조사 연구 최종 보고서", 2006.

[2] EPCglobal. "The EPCglobal architecture framework final version", July 1, 2005

[3] 정보통신연구진흥원. "역할기반 접근제어 컴포넌트 S/W개발 연구결과보고서", 2003.

[4] EPCglobal. "EPC Information Services(EPCIS) Version 1.0 Specification", April 12, 2007

[5] EPCglobal. "Object Naming Service(ONS) Version 1.0", October 4, 2005

[6] 한국유통물류진흥원. http://www.eankorea.or.kr/

[7] NIST(National Institute of Standards and Technology). "An Introduction to Role Based Access Control", December, 1995

[8] Ravi S. Sandhu, Edward J.Coyne, Hal L. Feinstein and Charles E. Youman, "Role-Based Access Control Models", IEEE Computer, Volume 29, Number2, pages 3847, February 1996.

[9] Ravi Sandhu and Hal Feinstein, "A Three Tier Architecture for Role-based Access Control", Proceedings of the 17th NIST-NCSC National Computer Security Conference, 1994. 10.

[10] Barkley, Cincotta, Ferraiolo, Gavrilla and Kuhn, "Role Based Access Control for the World Wide Web", 20th National Computer Security Conference, 1997.

[11] R.J.Hayton, J.M.Bacon, K.Moody. "Access Control in an Open Distributed Environment", Security and Privacy, 1998. Proceedings. 1998 IEEE Symposium, May, 1998

[12] Ralf Rantzau, Karin Kailing, Steve Beier, Tyrone Grandison. "Discovery Services—Enabling RFID Traceability in EPCglobal Networks", Proc. of the 13th International Conference on Management of Data (COMAD) 2006, Delhi, India. December 2006.

[13] B.Fabian, O.Güunther, and S.Spiekermann, "Security Analysis of the Object Name Service(ONS) for RFID", Security, Privacy and Trust in Pervasive and Ubiquitous Computing, July, 2005