협동조합을 위한 전자 페디그리 사설인증 방법

김상식* · 채명수* · 정성관*

*한국과학기술원 (KAIST) IT융합연구소

Private Certification Method of ePedigree for Cooperatives

Sangsik Kim* · Myungsu Chae* · Sungkwan Jung*

*Korea Advanced Institute of Science and Technology (KAIST) Institute for IT Convergence

E-mail : sskim98@itc.kaist.ac.kr · mschae89@itc.kaist.ac.kr · skjung@itc.kaist.ac.kr

요 약

제품과 유통과정의 정보들을 유통 파트너 상호간에 공유하는 것은 제품 유통 과정의 기본적인 활동이며 유통의 성공을 보장하는 핵심 요구사항이다. 제품의 생산자부터 리테일에 이르기까지의 모든 이벤트를 저장하는 페디그리는 유통 체인의 모든 주체에게 추적 가능한 정보를 저장하고 공유하는 유연한 메커니즘을 제공하고 Public Key Infrastructure(PKI) 기반의 디지털 서명을 이용하여 공유하는 정보의 신뢰성을 제공한다. PKI를 통해 인증 가능한 서명을 하기 위해서 유통 체인의 주체들은 Certificate Authority(CA)로부터 PKI 인증서를 구매해야만 한다. 다수의 영세 조합원들로 구성된 농축산 협동조합의 경우 구성원들 모두가 PKI 인증서를 구매하는 것은 현실적으로 어렵고 이 것은 페디그리가 유통과정에 적용되는 데 있어서 큰 장애요소이다. 본 논문은 협동조합을 위한 페디그리 사설 인증 방법을 제안한다. 협동조합은 제안하는 전자 페디그리를 최소의 비용으로 조합 전체에 적용 가능하며, 제안한 방법은 기존 전자 페디그리와 동일하게 정보의 신뢰성을 보장할 수 있다.

ABSTRACT

Sharing of product and process information with partners is a basic activity and key requirement which ensures success of distribution. ePedigree that encapsulates all of the event data from manufacturer to retail shop provides a flexible mechanism of storing and sharing traceable information to the partners of supply chain and credibility of shared information through digital signature based on Public Key Infrastructure (PKI). To generate the signature that can be authenticated through PKI, the partners of supply chain should pay for PKI certificates from Certificate Authority (CA). In case of agrifood cooperatives which consist of petty merchants or farmers, it is hard to pay for the PKI certificate for all members and is a big obstacle for the ePedigree to be applied to the supply chain. This paper proposes a private certification method of ePedigree for cooperatives. Cooperatives can apply the ePedigree using the proposed method to all the members at small cost and the proposed method can assure the credibility of information at the same level of the previous ePedigree.

키워드

협동조합, 전자 페디그리, 전자서명, 사설인증, 인증서

Ⅰ. 서 론

제품의 정품확인과 이력추적을 목적으로 기존 EPCglobal에서 개발된 페디그리(ePedigree)는 주로 의약품의 물류/유통 및 판매 과정에서 중요한 생산/유통 정보의 확인을 가능하게 하여 소비자의 의약품 복용시 안전성을 보장한다. 페디그리는 의약품의 물류/유통 과정에서 발생한 제품의 생산/유통 정보를 수집하여 페디그리에 저장하며

PKI 인증서로 서명하고 다음 유통 주체로 전달하는 과정을 통해 제품 안전성을 보장한다. 최근 전 세계적으로 농식품의 생산 및 유통과정에서 발생할 수 있는 식품 안전성 문제가 사회적 이슈로 대두되면서 페디그리는 농식품 안전성 문제를 해결할 하나의 방법으로 고려되고 있다.

페디그리는 기본적으로 페디그리의 서명 및 검증을 위해 PKI를 통한 PKI 인증서 발급 및 검증 절차를 요구한다. 그러나, 국내 협동조합의 경우 다수의 조합원들이 소규모 생산을 하기 때문에 페디그리 사용을 위해 PKI 인증서를 구매하는 것은 활용도 대비 너무 많은 비용을 발생시킨다. 이러한 비용 문제는 협동조합에 의한 제품 유통에 있어서 페디그리를 적용하기 어려운 가장 큰 요인이다. 국내 농식품 생산 및 유통에 있어서 협동조합의 비중이 상당하기 때문에 이러한 비용 문제를 해결하여 협동조합이 페디그리를 도입하고 안전한 제품을 소비자에게 제공할 수 있는 방법을 제공해야 한다.

본 논문은 제품의 안전한 생산/유통 정보 확인과 이력추적을 목표로 하는 기존 페디그리에 사설 인증서 발급 및 서명 검증 방법을 정의함으로써 페디그리의 유통분야 적용시 발생하는 비용 문제를 해결하고 공급망 구성원 간 제품 안전성 확보가 가능한 프로세스 및 요구사항을 제안한다.

II. 본 론

1. 관련 연구

페디그리가 제품의 유통과정에서 발생하는 다양한 정보를 기록하여 의약품의 제품 신뢰성 확보를 목적으로 개발됨으로써, 관련 연구도 주로 페디그리의 유통정보 역추적 기능을 활용한 제품 이력추적 방법, 유통정보 수집 범위 확장을 통한 제품 유통과정의 신뢰성 확보방법, 다양한 제품 유통 정보를 효율적으로 저장하고 제공하기 위한 시스템 성능 개선 방법 측면에서 진행되고 있다.

페디그리를 이용한 이력 추적의 경우 특수의약품[1][2] 및 보석[3] 유통 분야에 적용하여 RFID를 활용한 제품 유통정보 수집기능과 페디그리 진품인증 기능을 연동하여 유통과정의 이력정보를 제공하는 방법을 제안하고 있다. 이 연구들은 제품 유통과정에서 발생하는 이벤트 정보를 RFID 및 EPCIS를 통하여 수집하고, 이 정보를 기반으로 페디그리를 작성하여 제품 이동시 전달함으로써 안전한 제품 유통 및 이력 정보 제공을 위한 방법을 제안하고 있다.

페디그리 정보 확장을 통한 제품 유통과정 신뢰성 확보 연구의 경우 의약품[4][5], 급식[6], 농산물[7][8][9] 등 다양한 응용 분야에서 연구되고 있으며, 주로 새로운 수집정보를 정의하여 페디그리에 적용하기 위한 페디그리 필드 확장 관련 연구들이 진행되고 있다. 기존 페디그리가 제품의 기본 정보만 저장하고 있는 반면, 이 연구들은 다양한 제품 분야의 유통 과정에서 발생하는 환경정보, 위치정보, 보관정보 등 유통 정보를 페디그리에 기록하여 제품의 유통과정에서의 신뢰성을 확보하는 방법을 제안하고 있다. 또한, 페디그리 시스템의 성능개선 관련연구의 경우 효율적인 페디그리 위변조 감지를 위한 시스템 구조 및 알고리즘[10]을 제안하거나, 페디그리가 수KB 내외의 작은 정보 단위로 기록되고 수백만 단위의 페디그리들이 저장되기 때문에 효율적인 저장소 관리를 위한 하둡기반 페디그리 시스템 성능 개선 방법[11] 등이 있다.

기존의 연구들은 주로 실제 유통체인에 페디그리 시스템을 적용하기 위하여 시스템이 갖추어야 할 기능 및 성능 측면에서의 요구사항을 정의하고 개선 방안을 제안하고 있다. 그러나 항상 이윤 극대화를 추구하는 유통체인의 기본 특성을 고려하면 페디그리 시스템은 유지비용 측면에서도 필요한 요구사항 정의 및 시스템 구조 개선이 필요하다. 본 논문에서는 페디그리 시스템의 기본 비용 요구사항인 인증서 비용 문제를 해결함으로써 페디그리 시스템이 보다 쉽게 유통체인에 적용될 수 있는 방법을 제안한다.

2. 페디그리 사설인증 방법

이 단락에서는 제품 생산 및 유통 과정의 정보를 기록하기 위한 사설 인증 페디그리의 형식과 세부 필드 내용에 대해 정의한다. 사설 인증 페디그리는 GS1 “Pedigree Ratified Standard”[1]의 내용을 포함하며 사설 인증을 위한 필드들을 추가적으로 포함한다.

페디그리는 그림 1과 같이 다양한 유통 주체를 경유하여 유통 이벤트 정보들을 저장하게 되며, PKI 인증과 사설 인증을 통해 작성된 페디그리에 대한 부인 방지가 수행된다. 페디그리를 생성 또는 갱신한 페디그리 서버는 고유의 개인키로 서명하여 페디그리의 내용을 해당 서버에서 작성하였음을 보증한다. 다른 페디그리 서버 또는 소비자 단말로부터의 요청이 있을 때 인증서를 응답함으로써 페디그리의 유효성 검증이 이루어진다.

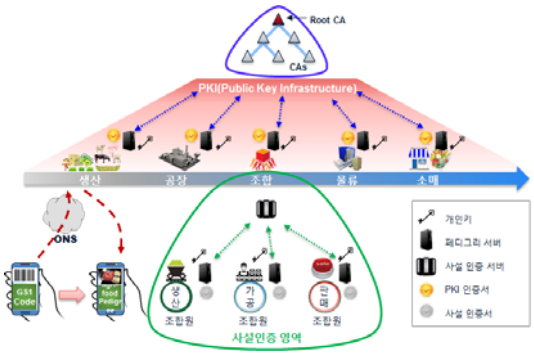


그림 1. 페디그리 인증 시스템

페디그리의 서명 및 인증을 위하여 모든 페디그리 서버는 개인키와 인증서를 가진다. 모든 페디그리는 페디그리 서버의 개인키로 서명되어야 하며 페디그리에 대한 검증이 필요한 경우 인증서를 이용하여 검증을 수행한다. 인증서는 PKI 인증서와 사설 인증서가 될 수 있으며 PKI를 통한 인증 방법은 RFC3280에 기술되어 있으므로 본 논문에서는 사설 인증 방법에 대해 다룬다. 본 단락에서는 사설 인증을 위한 사설 인증 페디그리 형식과 추가되는 세부 필드에 대해 정의한다.

그림 1에서 조합 내의 구성원들은 사설인증 방법을 사용함으로써 전체 유통체인은 조합을 기준으로 PKI 인증과 사설인증의 영역이 구분된다. 조합 내부에서 생성된 사설 인증서는 조합 외부의 페디그리 서버에서 그 유효성이 검증될 수 없으므로, 조합 내에서 생성된 페디그리들은 항상 조합의 페디그리 서버를 경유하여 조합 외부로 전달되고 그때 조합의 페디그리 서버가 페디그리의 유효성을 보증하기 위한 정보를 페디그리에 삽입함으로써 조합의 페디그리 서버가 모든 조합 내 페디그리의 유효성을 보증하는 형태로 사설인증 페디그리 시스템이 동작한다.

조합의 페디그리 서버는 조합 내에서 생성된 페디그리를 수신할 때 receivedPedigree를 생성하고 receivingInfo에 privateDocumentInfo 필드를 두어 조합원으로부터 수신한 사설 인증 페디그리가 사설 인증이 필요한 페디그리임을 명시한다. 그림 2와 표 1은 협동조합 외부에서 사설 인증을 수행할 때 이용될 정보를 담고 있는 확장된 receivingInfoType과 privateDocumentInfo 필드에 대한 정의이다.

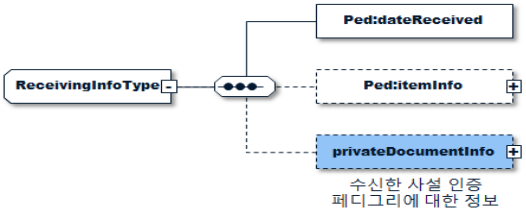
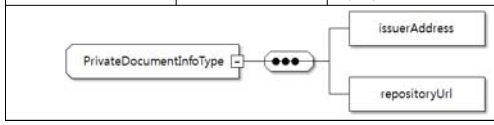


그림 2. 사설인증 페디그리 receivingInfo 요소

표 1. privateDocumentInfo 데이터 요소

구성 요소	타입	설명
issuerAddress	ContactType	사설 인증 서버를 운영하는 기관정보
repositoryUrl	xs:string	사설 인증을 위해 접근할 사설 인증 서버 URL 정보
		

privateDocumentInfo 의 내용으로 조합 페디그리 서버는 signerInfo에 따라 issuerAddress를 ContactType으로 작성하여 조합의 정보를 기록하고 수신한 페디그리의 사설 검증을 위한 repositoryUrl 주소를 기록한다. 조합에서 전달된 사설 인증 페디그리를 수신한 조합 외부의 페디그리 서버는 사설 인증 페디그리의 검증을 수행할 수 있다. 사설 인증 페디그리 검증 과정에서 receivedPedigree 내 privateDocumentInfo가 발견되면 receivedPedigree 내에 포함된 사설 인증 페디그리 들은 issuerAddress에 해당하는 조합에서 보증하는 것으로 간주한다.

조합 외부의 페디그리 서버는 페디그리 검증을 위하여 repositoryUrl로 접근하여 사설 인증 페디그리의 사설 인증에 필요한 사설 인증서를 수신하고 사설 인증 페디그리를 인증한다. privateDocumentInfo가 발견되지 않는 다면 페디그리 서버는 페디그리를 PKI를 통해서 인증한다.

페디그리의 사설인증 절차는 다음과 같다.

1. privateDocumentInfo가 발견되면 issuerAddress의 정보가 receivedPedigree의 signerInfo와 동일한지 확인한다. 동일한 경우에만 인증 절차를 진행한다.
2. receivedPedigree내 페디그리들을 인증하기 위해 페디그리 서버는 TLS 연결을 통해 repositoryUrl에 접근하여 조합 사설 루트 인증서를 응답받는다.
3. repositoryUrl로 접근할 때 파라미터로서 각 사설인증 페디그리 내 signerInfo의 name 필드와 signatureDate를 전송한다.
4. repositoryUrl을 통한 사설 인증의 대상 페디그리는 privateDocumentInfo가 발견된 페디그리에 포함된 첫 번째 페디그리부터 issuerAddress와 동일한 이름의 signerInfo를 포함하는 페디그리까지의 모든 페디그리로서 모든 사설 인증 대상 페디그리에 대하여 반복하여 인증을 수행한다.

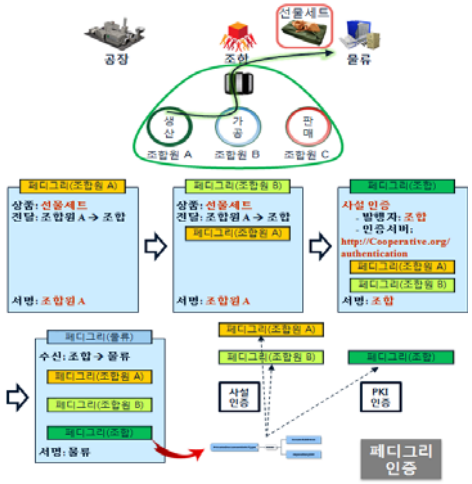


그림 3. 사설인증 필드에 의한 인증과정

3. 페디그리 사설인증 시스템 구현

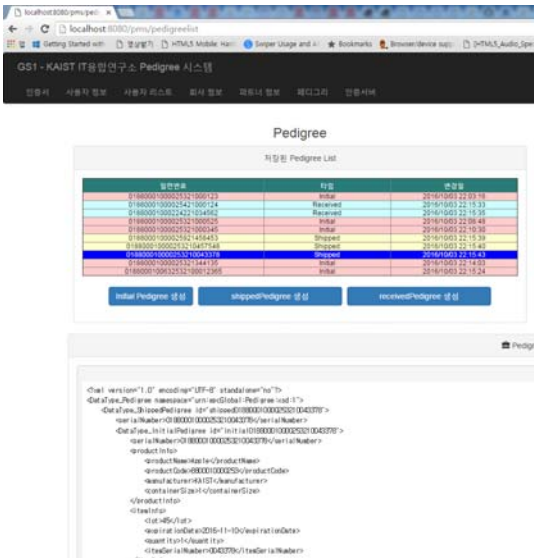


그림 4. 페디그리 시스템 제어 화면

본 논문의 사설인증 기반 페디그리 시스템은 스프링 프레임워크 기반의 환경에서 자바 웹 서비스로서 개발되었다. 개발된 페디그리 시스템은 몽고디비를 사용하며 아파치 톰캣 상에서 동작 가능하다. 개발된 페디그리 시스템은 PKI 인증서와 사설 인증서를 모두 지원하며 InitialPedigree, ShippedPedigree, ReceivedPedigree의 생성, 페디그리 서명 및 페디그리 시스템 간 TLS 기반 페디그리 전송, 페디그리 서명 검증, 인증서 검증, 인증서 경로 검증의 기능이 구현되어 있다.

또한, 페디그리 시스템을 이용하는 사용자 관리, 파트너 관리, 회사정보 관리, 페디그리 및 인증서 관리 등의 기능이 구현되어 유통체인에서 즉시 활용 가능하도록 개발되어 있다.

III. 결 론

본 논문은 제품의 생산/유통 정보 확인과 이력 추적을 목표로 하는 기존 페디그리에 사설 인증 방법을 정의함으로써 페디그리 시스템의 유통분야 적용시 발생하는 비용 문제를 해결하고 공급망 구성원 간 정보 공유를 위한 사설인증 페디그리 전송 프로세스 및 요구사항을 제안하였다. 본 논문의 사설인증 페디그리는 기존 페디그리 시스템의 최소한의 변경으로 기능 구현이 가능하도록 설계되었다. 개발된 사설인증 페디그리 시스템은 실제 유통에서 저비용으로 페디그리 시스템 운용하는 데 도움을 줄 것으로 예상된다.

사사표기

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. R0126-16-1002, Development of agro-livestock cloud and application service for balanced production, transparent distribution and safe consumption based on GS1)

참고문헌

[1] M. Solanki and C. Brewster, “EPCIS Event-Based Traceability in Pharmaceutical Supply Chains via Automated Generation of Linked Pedigrees,” ISWC, LNCS 8796, pp. 82-97, Oct. 2014.

[2] 이봉근, “RFID 기반의 특수의약품 추적관리 시스템 설계 및 구현,” 정보처리학회논문지, Part D, pp. 977-984, Dec. 2006.

[3] 안혜정, 박현규, 이종태, “이력 및 진품확인을 지원하는 진주보증시스템 설계 및 구현,” 대한산업공학회 춘계공동학술대회 논문집, pp. 233-240, 2008.

[4] 서동민, 정해준, 김현수, “의약품 정품인증 및 품질 추적을 위한 e-pedigree 연구,” 로지스틱스연구, 19권. 1호, pp. 141-157, 2011.

[5] 김동진, 김현수, 이종민, 한정훈, “의약품 공급망의 확장형 페디그리 적용에 따른 데이터량에 관한 연구,” 로지스틱스연구, 21권. 3호, pp. 107-120, 2013.

[6] 김현수, 정해준, “콜드체인 공급사슬 이력추적 관리모델,” 한국 SCM 학회지, 13권. 2호, pp. 87-97, Oct. 2013.

[7] W. Han, *et al.*, “The design of an electronic pedigree system for food safety,” Information Systems Frontiers, Vol. 17, pp. 275-287, Apr. 2015.

[8] 안혜정, G. Alfian, U. Farooq, M. A. Syaekhoni, 한정훈, 이종태, “효율적인 농산물 콜드체인을 위한 국제 표준 기반의 e-페디그리 모형 설계,” 대한산업공학회 춘계공동학술대회 논문집, pp. 956-963, May. 2014.

[9] U. Farooq, G. Alfian, M. A. Syaekhoni, H. Ahn, J. Rhee, “A Centralized e-pedigree system for Agriculture Food Distribution Network,” 대한산업공학회 춘계공동학술대회 논문집, pp. 964-970, May. 2014.

[10] S. H. Choi, *et al.*, “ Implementation issues in RFID-based Anti-counterfeiting for Apparel Supply Chain,” IJICR, Vol. 5, pp. 379-389, Dec. 2014.

[11] Y. Zhang, et al., “Optimizing the Storage of Massive Electronic Pedigrees in HDFS,” IOT, pp 68-75, 2012.