TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx/R1 제(개)정일: 20xx년 xx월 xx일

협동조합을 위한 페디그리(pedigree) 사설 인증 방법

Private Certification Method of Pedigree for Cooperative

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 스마트통업 프로젝트그룹(PG426)

표준안 심의 위원회 정보기술 융합 기술위원회(TC4)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	김상식	KAIST	선임연구원	-	
	김대영	KAIST	교수	스마트농업PC위원	
표준 초안 작성자	김상식	KAIST	선임연구원	-	
	김대영	KAIST	교수	스마트농업PC위원	
사무국 담당				-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx

서 문

1 표준의 목적

본 표준은 협동조합을 위한 페디그리(pedigree)의 생성/갱신 및 인증 방법에 대해 정의한다. 협동조합의 특성에 맞추어 기존 의약품용 페디그리를 확장하고 조합원을 위한 사설 인증 방법을 정의하여 제품 유통과정에서 페디그리가 안전하고 효과적으로 이용될 수 있도록 한다.

2 주요 내용 요약

현재의 페디그리 표준은 주로 의약품의 유통을 위한 요구사항을 정의하고 있다. 엄격한 페디그리 정보 관리를 위해, 의약품 페디그리는 PKI(public key infrastructure)를 통한 PKI 인증서로 서명되며 PKI를 통해 검증된다. 이 표준들을 협동 조합 분야에 적용할 경우 협동조합 내 모든 조합원들은 CA(Certificate Authority)를 통하여 PKI 인증서를 구매해야 한다.
협동조합의 경우 다수의 조합원들이 소규모 생산을 하기 때문에 페디그리 사용을 위해 PKI 인증서를 구매하는 것은 활용도 대비 너무 많은 비용을 발생시킨다. 본 표준은 사설 인증서를 활용한 페디그리 요구사항을 정의하고 이렇게 만들어진 페디그리의 인증을 위한 인터페이스를 정의한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준은 EPCglobal, “Pedigree Ratified Standard”, January 2007.을 기반으로 하는 페디그리의 사설 인증 방법을 정의한다. 본 표준은 사설 인증을 위한 추가적인 페디그리 필드, 사설 인증 서버 요구사항, 사설 인증 절차 요구사항을 정의한다.

3.2 인용 표준과 본 표준의 비교표

TTAK.xx-xx.xxxx/R1	"Pedigree Ratified Standard" version 1.0	비고
1. receivedPedigree 규격	1. receivedPedigree 규격	동일
2. privateDocumentInfo	-	추가
3. issuerAddress	-	추가
4. repositoryUrl	-	추가

Preface

('서문' 중 아래 항목을 영문으로 작성)*

1 Purpose

This standard defines the methodologies of create, update and certify pedigree for cooperative. it enables existing pedigree of medical supplies to extend based on characteristics of cooperative, and to be used safe and effective in circulation process by defining methodologies of private certification for union members.

2 Summary

Current pedigree standards define mainly about requirements for circulation of medical supplies. For strict rarity certification, pedigree of medical supplies is signed through public key infrastructure (PKI) certificate and also verified through PKI. Once these standards are applied to cooperatives, all of producer and distributor should buy the PKI certificate through certificate authority (CA).
Since lots of producers produce small amount in cooperative, purchasing PKI certificate for using pedigree induces relatively high costs comparing to utilization. This standard defines requirements of pedigree applying private certificate and interface for certifying the pedigree.

3 Relationship to Reference Standards

This standard defines the methodologies of private certification for the pedigree which is based on EPCglobal, "Pedigree Ratified Standard", January 2007. The standard defines additional pedigree fields, requirements of private certification server, requirements of private certification procedures for private certification.

목 차

1 적용 범위 ····· 1

2 인용 표준 ····· 1

3 용어 정의 ····· 1

4 약어 ····· 2

5 개요 ····· 3

6 사설 인증 페디그리 ····· 4
6.1 사설 인증 페디그리 형식 ····· 5

7 사설 인증 페디그리 ····· 7

8 페디그리 서버 요구사항 ····· 9
8.1 페디그리 서버 요구사항 1: 인증서 발급 및 서명 ····· 9
8.2 페디그리 서버 요구사항 2: 사설 인증 서버 운영 및 PKI 인증서 사용 ····· 9
8.3 페디그리 서버 요구사항 3: privateDocumentInfo 기록 ····· 10
8.4 페디그리 서버 요구사항 4: 사설 인증 페디그리 인증 ····· 10

9 사설 인증 절차 요구사항 ····· 11

10 사설 인증 절차 요구사항 ····· 13
10.1 조합 내 생산품의 유통과 인증 ····· 13
10.2 조합 내 가공품의 유통과 인증 ····· 13

부록 Ⅰ-1 지식재산권 확약서 정보 ····· 15
Ⅰ-2 시험인증 관련 사항 ····· 16
Ⅰ-3 본 표준의 연계(family) 표준 ····· 17
Ⅰ-4 참고 문헌 ····· 18
Ⅰ-5 영문표준 해설서 ····· 19
Ⅰ-6 표준의 이력 ····· 20

협동조합을 위한 페디그리(pedigree) 사설 인증 방법
(Private Certification Method of Pedigree for Cooperative)

1 적용 범위

이 표준은 협동조합의 안전하고 효율적인 페디그리 운용을 위한 페디그리 요구사항을 정의한다. 본 표준에서 협동조합은 사설 인증서를 발급하여 조합원의 PKI 인증서 구매 비용을 절약할 수 있다. 또한, 페디그리의 서명을 검증하기 위한 표준화된 인터페이스를 제공함으로써 안전한 페디그리 운용을 가능하게 한다. 조합을 통한 제품 유통에 있어서 페디그리 시스템이 적용되기 어려운 이유 중 하나는 높은 인증서 구매 비용이다. 본 표준은 저비용 페디그리 운용 방법을 제안하여, 협동조합이 관여하는 유통산업에의 페디그리 적용을 유도하고 소비자에게는 더욱 안전한 제품을 제공하도록 한다.

2 인용 표준

- EPCglobal, Pedigree Ratified Standard, version 1.0, January 2007.

3 용어 정의

3.1 사설 인증 페디그리

사설 인증 페디그리(private certification pedigree)는 기존의 의약품용 페디그리를 사설 인증이 가능하도록 확장한 페디그리로서 기본적으로 의약품용 페디그리와 동일하게 유통 과정에서 발생하는 다양한 이벤트 정보를 기록하며 유통 주체간 송수신을 통해 제품의 안전성을 보장하는 페디그리 정보이다. 사설 인증 페디그리는 기존 의약품용 페디그리와 동일하게 제품 정보, 트랜잭션 정보, 공급자 정보, 구매자 정보, 서명을 포함하며 추가적으로 사설 인증을 지원하기 위한 확장 정보를 포함한다.

3.2 페디그리 서버

페디그리 서버는 페디그리의 생성 및 유통 주체간 송수신을 위해 유통 주체에서 운영하는 관리 서버로 EPCIS의 이벤트 또는 페디그리 서버 관리자의 요청을 수신하여 페디그리 생성, 전송, 수신, 업데이트를 수행하는 시스템이다. 또한 페디그리 서버는 생성, 수신, 업데이트를 수행한 모든 페디그리를 내부에 저장하며 임의의 GS1 코드에 대한 페디그리 검색 요청에 대하여 저장소를 검색하여 페디그리를 응답한다.

3.3 사설 인증서

사설 인증서는 페디그리 서버에 의해 운영되는 사설 인증 서버에서 발행된 인증서이다. PKI 인증서의 경우 PKI의 CA에 의해 서명된 공개키를 포함하며 CA에 의해 발행되지만 사설 인증서의 경우 사설 인증 서버에서 서명된 공개키를 포함하며 사설 인증 서버를 통해 검증되는 인증서이다.

3.4 사설 인증 서버

사설 인증 서버는 페디그리 서버에서 운영하는 인증서 관리 서버이다. 사설 인증 서버는 페디그리 서버의 요청이 있을 때 공개키에 대하여 서명하는 것으로 사설 인증서를 발행하고 외부의 요청이 있을 때 사설 인증서를 제공한다.

4 약어

PKI	Public Key Infrastructure
CA	Certificate Authority
EPCIS	Electronic Product Code Information Services
GS1	Global Standard #1
PCP	Private Certification Pedigree

5 개요

제품의 정품확인과 이력추적을 목적으로 기존 EPCglobal에서 개발된 페디그리(ePedigree) 표준은 주로 의약품의 물류/유통 및 판매 과정에서 중요한 생산/유통 정보의 확인을 가능하게 하여 소비자의 의약품 복용시 안전성을 보장한다. 페디그리 표준은 의약품의 물류/유통 과정에서 제품의 정보를 페디그리로 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 페디그리 표준은 농식품 안전성 문제를 해결할 하나의 방법으로 고려되고 있다.

페디그리 표준은 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 페디그리 시스템을 적용하기 어려운 가장 큰 요인이다. 국내 농식품 생산 및 유통에 있어서 협동조합의 비중이 상당하기 때문에 이러한 비용 문제를 해결하여 협동조합이 페디그리 시스템을 도입하고 안전한 제품을 소비자에게 제공할 수 있는 방법을 제공해야 한다.

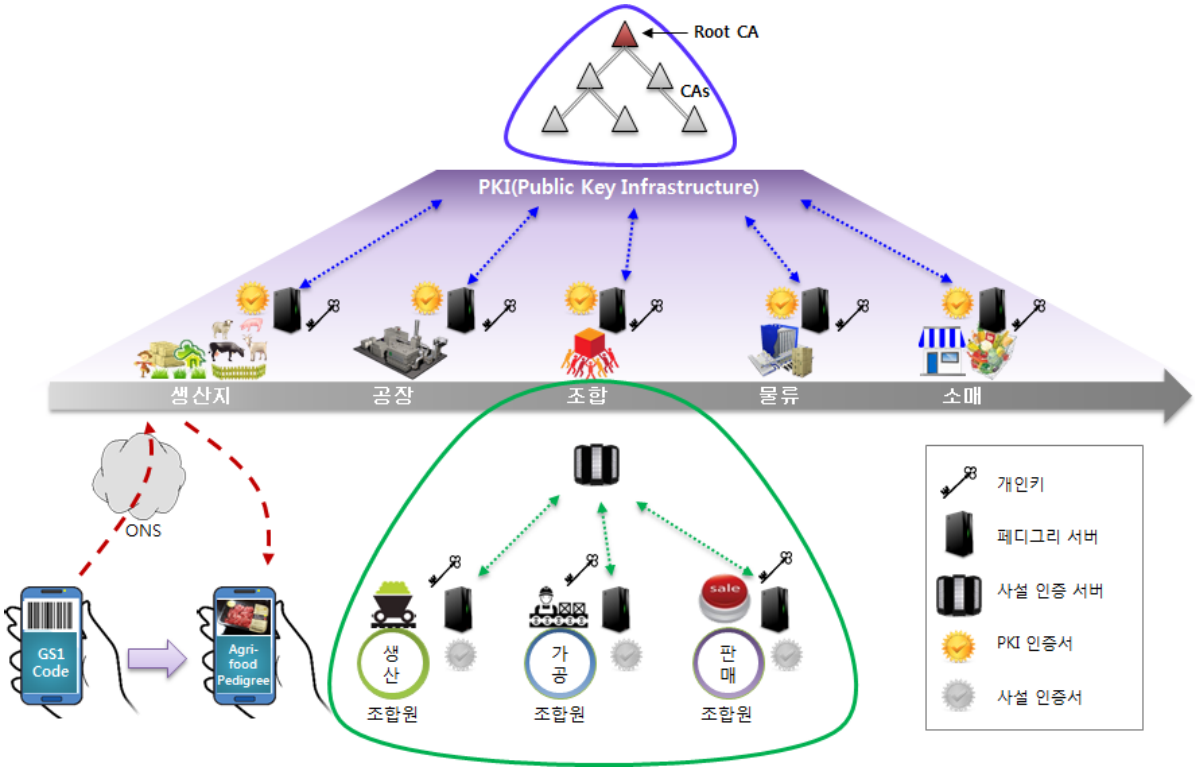
본 표준은 제품의 안전한 생산 및 유통 정보 확인과 이력추적을 목표로 하는 기존 페디그리 표준 기반에 사설 인증서 발급 및 서명 검증 방법을 정의함으로써 페디그리 시스템의 유통분야 적용시 발생하는 비용 문제를 해결하고 공급망 구성원 간 제품 안전성 확보가 가능한 프로세스 및 요구사항을 표준으로 제안하고자 한다.

6 사설 인증 페디그리

이 단락에서는 제품 생산 및 유통 과정의 정보를 기록하기 위한 사설 인증 페디그리의 형식과 세부 필드 내용에 대해 정의한다. 사설 인증 페디그리는 "Pedigree Ratified Standard" version 1.0의 내용을 포함하며 사설 인증을 위한 필드들을 추가적으로 포함한다.

페디그리는 그림 6-1과 같이 다양한 유통 주체를 경유하여 유통 경로상의 이벤트 정보들을 저장하게 되며, PKI 인증과 사설 인증을 통해 작성된 페디그리에 대한 부인 방지가 수행된다. 페디그리를 새롭게 생성 또는 갱신한 페디그리 서버는 고유의 개인키로 서명하는 과정을 통해 페디그리의 내용을 해당 페디그리 서버에서 작성하였음을 보증한다. 다른 페디그리 서버 또는 소비자 단말로부터의 요청이 있을 때 PKI 또는 사설 인증 서버에서 페디그리 서버 인증서를 전달해 주는 과정을 통해 페디그리의 유효성 검증이 이루어진다.

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 표준에서는 사설 인증 방법에 대해 다룬다. 본 단락에서는 사설 인증을 위한 사설 인증 페디그리 형식과 추가되는 세부 필드에 대해 정의한다.

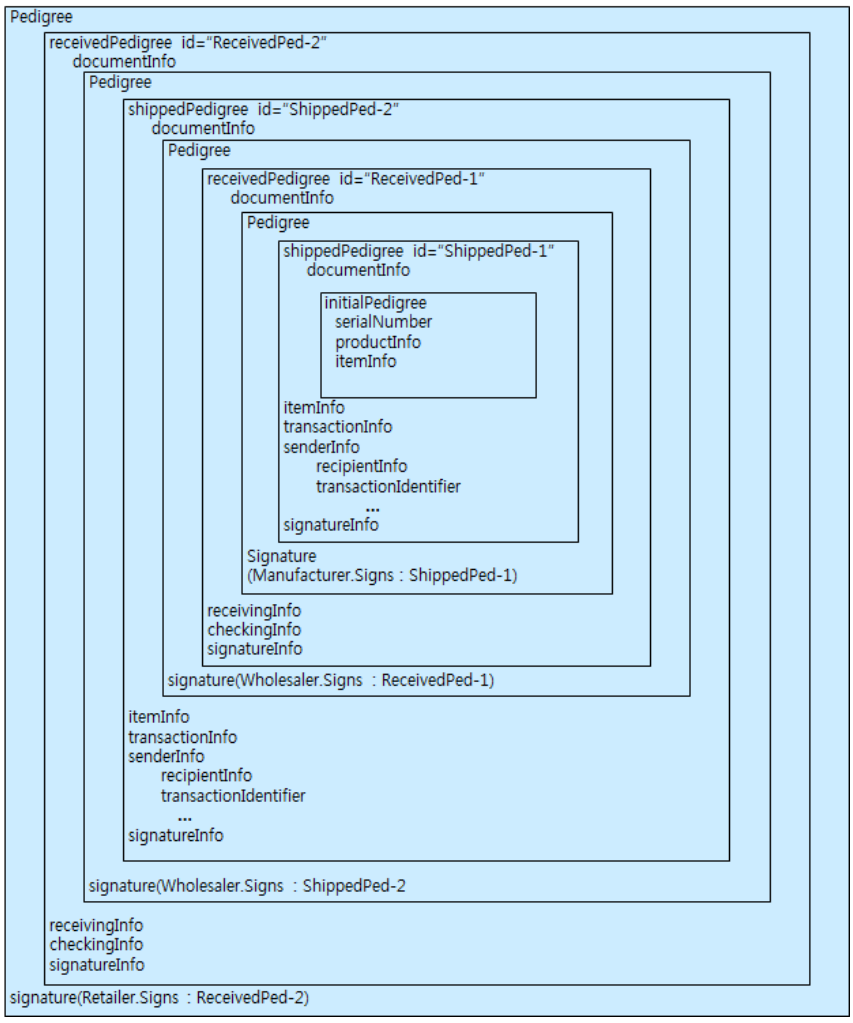


(그림 6-1) 페디그리 인증 시스템

6.1 사설 인증 페디그리 형식

사설 인증 페디그리 형식은 그림 6-2와 같이 "Pedigree Ratified Standard" version 1.0에 기술된 e-pedigree 형식을 따른다. 본 단락에서는 e-pedigree 형식에 협동조합 내부에서 생성 및 갱신되는 사설 인증 페디그리의 사설 인증을 위해 새롭게 정의되는 필드에 대해 기술한다.

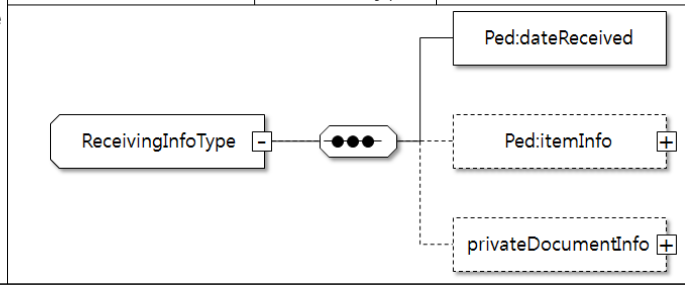
협동조합 내부 조합원이 사설 인증 가능한 사설 인증 페디그리를 생성 및 갱신 할 수 있도록 하고 조합 외부에 사설 인증 기능을 제공하기 위하여 조합원과 외부 파트너사 간의 모든 거래는 반드시 조합을 경유하여야 함을 정의한다. 즉, 조합원이 생성 및 갱신한 사설 인증 페디그리는 반드시 협동조합 페디그리 관리서버에 전송되고 외부에서 전달되는 페디그리는 반드시 협동조합 관리서버를 경유하여 조합원에게 전달된다. 협동조합 페디그리 서버는 외부에서 전달되는 페디그리를 내부로 전달할 때 전달된 페디그리를 감싸는 shippedPedigree를 생성하며 내부에서 생성 및 갱신된 페디그리를 외부로 전달할 때 receivedPedigree를 생성하여 이전에 수신한 페디그리를 포함시킨다.



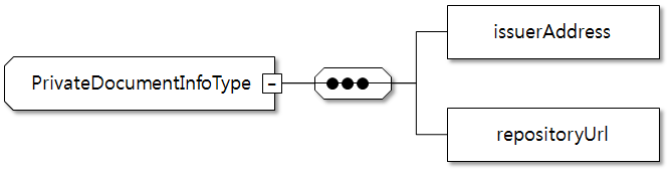
(그림 6-2) 페디그리 형식

협동조합 페디그리 서버는 receivedPedigree를 생성할 때 receivingInfo에 privateDocumentInfo 필드를 두어 조합원으로부터 수신한 사설 인증 페디그리가 사설 인증이 필요한 페디그리임을 명시한다. 표 6-1과 6-2는 협동조합 외부에서 사설 인증을 수행할 때 이용될 정보를 담고 있는 확장된 receivingInfoType과 privateDocumentInfo 필드에 대한 정의이다.

<표 6-1> 사설 인증 페디그리의 receivingInfo 데이터 요소

데이터 요소	데이터 타입	구성 요소	타입	설명
receivingInfo	ReceivingInfoType	dateReceived	xs:date	아이템이 도착한 날짜
		itemInfo	ItemInfoType	사설 인증 페디그리와 연관된 실제 아이템에 대한 정보.
		privateDocumentInfo	PrivateDocumentInfoType	수신한 사설 인증 페디그리에 대한 정보
				

<표 6-2> 사설 인증 페디그리의 privateDocumentInfo 데이터 요소

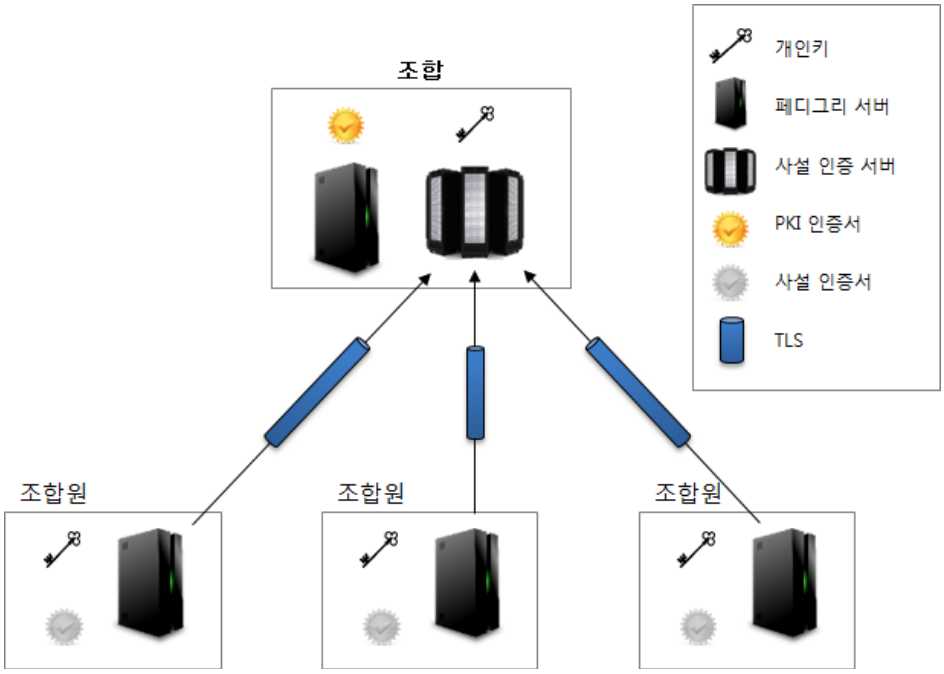
데이터 요소	데이터 타입	구성 요소	타입	설명
privateDocumentInfo	privateDocumentInfoType	issuerAddress	ContactType	사설 인증 서버를 운영하는 협동조합의 정보
		repositoryUrl	xs:string	사설 인증을 위해 접근할 사설 인증 서버 URL 정보
				

협동조합의 페디그리 서버에서 privateDocumentInfo 데이터 요소를 작성하여 외부로 사설 인증 페디그리를 전달한 경우 조합 외부에서는 이 데이터 요소를 이용하여 사설 인증을 진행할 수 있다. 자세한 사설 인증 방법은 9장 사설 인증 절차 요구사항에서 다룬다.

7 사설 인증 서버 요구사항

본 단락에서는 협동조합 내 조합원이 사설 인증 페디그리를 서명할 수 있도록 사설 인증서를 발행하고 외부의 요청에 의해 인증서를 제공하는 사설 인증 서버의 요구사항에 대해 기술한다.
사설 인증 서버는 농축산 협동조합 내 조합원들을 위해서 사설 인증서를 발행하고 인증서 저장소를 운영하는 서버이다. 사설 인증 서버는 다음과 같은 요구사항을 가진다.

- 조합원을 위한 사설 인증서를 발행할 수 있어야 한다.
- 페디그리 검증을 위한 인증서 요청에 대해 내부 저장소를 검색하여 인증서를 전송해야한다.
- 인증서 발행과 요청을 위한 연결은 TLS로 보호되어야 한다.
- TLS 연결을 위한 사설 인증 서버의 인증서는 PKI 인증서를 사용해야 한다.



(그림 7-1) 협동조합 및 조합원 간 인증서 관리 시스템

조합원을 위한 사설 인증서는 ITU-T X.509(ISO/IEC 9594-8) 인증서를 사용한다. 인증서 발행을 위한 과정으로 조합원의 페디그리 서버는 개인키를 생성하여 저장하고 사설 인증서버로 CSR(Certificate Signing Request)을 전달한다. 협동조합 사설 인증 서버 관리자는 CSR를 수신한 경우 조합 내부의 조합원 식별 과정을 통하여 CSR을 전송한 조합원을 식별한 후 조합원을 위한 사설 인증서를 발행한다.
조합원은 생성한 개인키를 이용하여 사설 인증 페디그리에 대하여 서명을 작성한다. 서명된 페디그리가 조합을 거쳐 조합 외부 페디그리 서버에 전송된 경우 조합 외부 페디그리 서버는 조합원의 인증서를 요청할 수 있다. 이 요청에 응답하기 위하여 사설 인증 서

버는 조합원의 모든 인증서를 저장하는 인증서 저장소를 운영하고 요청에 대하여 조합원의 인증서를 전달해야 한다.

모든 인증서 발행, 사설 인증서 요청에 대한 응답을 수행하면서 사설 인증 서버는 반드시 신뢰될 수 있어야 한다. 그러므로 사설 인증 서버는 반드시 PKI 인증서를 발급받아야 하고 TLS 연결에 대하여 PKI 인증서를 사용해야 한다. 또한 사설 인증 서버는 조합원의 사설 인증서 발행시 반드시 PKI 인증서를 발급받을 때 사용했던 개인키로 서명해야 한다.

8 페디그리 서버 요구사항

본 단락에서는 사설 인증 페디그리를 생성 및 갱신, 송수신하는 페디그리 서버의 요구사항에 대해 기술한다. 페디그리 서버는 제품 생산 및 유통 주체들에 의해 운영되는 페디그리 관리 서버이다. 페디그리 서버는 기본적으로 "Pedigree Ratified Standard" version 1.0에 기술된 e-pedigree를 생성 및 갱신하여 페디그리 서버 간 송수신 할 수 있어야 한다. 본 단락에서는 사설 인증 페디그리 이용을 위해 추가적으로 요구되는 사설 인증 관련 내용을 기술한다. 페디그리 서버 요구사항은 다음과 같다.

- 페디그리 서버는 PKI 또는 사설 인증서 중 어느 하나를 발급 받고 개인키를 이용하여 페디그리를 서명하여야 한다.
- 협동 조합을 위한 페디그리 서버는 사설 인증을 위해 사설 인증 서버를 운영해야 하며 페디그리 서버와 사설 인증 서버는 PKI 인증서를 사용해야 한다.
- 협동조합의 페디그리 서버는 조합 내 조합원이 운영하는 페디그리 서버로부터 사설 인증 페디그리를 수신하였을 때 receivedPedigree을 생성하고 privateDocumentInfo 항목을 기록하여야 한다.
- 페디그리 서버는 페디그리에 대하여 PKI 또는 사설 인증 서버를 통해 인증할 수 있어야 한다.

8.1 페디그리 서버 요구사항 1: 인증서 발급 및 서명

페디그리 서버는 협동조합 내 조합원에 의해 운영되는 페디그리 서버와 그 외 생산/유통 주체에 의해 운영되는 페디그리 서버로 나뉜다.
조합원에 의해 운영되는 페디그리 서버는 사설 인증서를 사용하고 그 외의 경우는 모두 PKI 인증서를 사용해야 한다. PKI 인증서를 사용하는 페디그리 서버는 관리자에 의해 개인키 및 PKI 인증서를 페디그리 서버에 입력할 수 있어야 한다.
사설 인증서를 사용하는 페디그리 서버는 개인키를 생성할 수 있어야 하며 개인키를 이용하여 CSR를 생성 후 사설 인증 서버로 전달할 수 있어야 한다. 또한, 사설 인증서를 이용하는 페디그리 서버는 사설 인증 서버로부터 발행된 인증서를 저장할 수 있어야 한다. 사설 인증 페디그리를 위한 사설 인증서는 최대 1년의 유효기간을 가지고 페디그리 서버는 관리자의 요청에 따라 언제든지 개인키 인증서 재발행을 할 수 있어야 한다.
페디그리 서버는 생성 및 갱신하는 모든 페디그리에 대하여 저장된 개인키를 이용하여 서명해야 한다.

8.2 페디그리 서버 요구사항 2: 사설 인증 서버 운영 및 PKI 인증서 사용

협동조합의 페디그리 서버는 조합 내 조합원에서 운영하는 페디그리 서버를 위한 사설 인증 기능을 제공하는 사설 인증 서버를 운영해야 한다.
협동조합 외부에서 조합 내부의 사설 인증을 기반으로 서명한 사설 인증 페디그리를 신

뢰하기 위한 조건은 협동조합의 페디그리 서버가 반드시 신뢰되고 조합 내부에서 생성/갱신된 사설 인증 페디그리를 조합의 페디그리 서버에서 receivedPedigree 생성을 통해 서명하는 것이다. 협동조합의 페디그리 서버가 반드시 신뢰되고 서명한 내용이 신뢰받을 수 있도록 하기 위하여 협동조합의 페디그리 서버는 PKI 인증서를 발급받아 사용해야 한다. 또한, 조합 외부에서는 조합 내부에서 생성된 사설 인증 페디그리의 서명을 검증하기 위해 사설 인증 서버로 접근했을 때 사설 인증 서버의 신뢰해야 하므로 사설 인증 서버도 PKI 인증서를 사용해야만 한다.

8.3 페디그리 서버 요구사항 3: privateDocumentInfo 기록

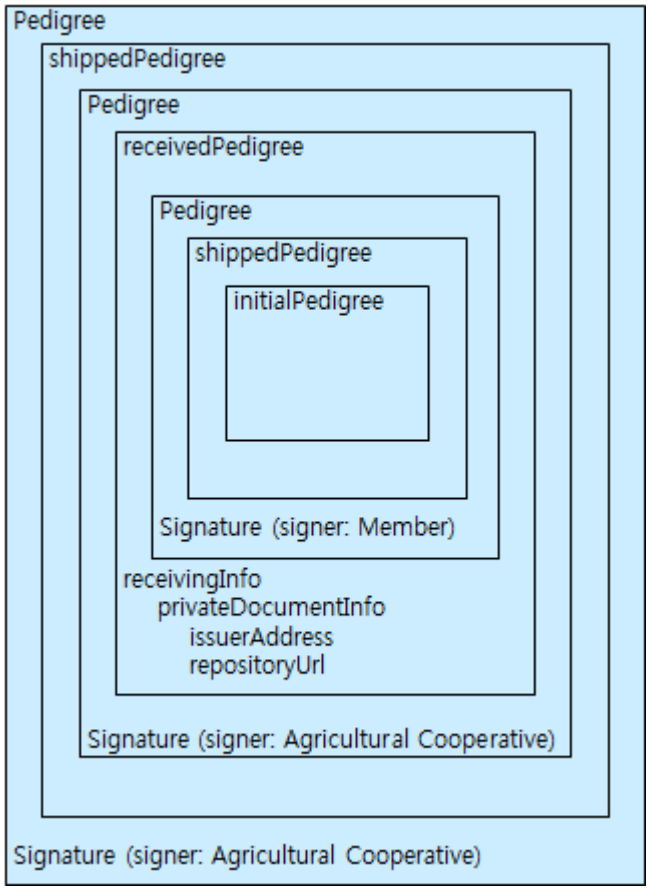
협동조합의 조합원에 대한 신원은 조합에서 보증하는 것처럼 사설 인증을 기반으로 조합원의 페디그리 서버가 서명한 사설 인증 페디그리의 신뢰성은 협동조합의 페디그리 서버가 보증한다. 조합 내에서 생성/갱신된 사설 인증 페디그리에 대한 신뢰성을 보장하기 위하여 조합의 페디그리 서버는 조합 내에서 생성/갱신된 사설 인증 페디그리가 외부로 전달 될 필요가 있을 때 receivedPedigree를 생성하고 privateDocumentInfo 내용을 기록해야만 한다. privateDocumentInfo 의 내용으로 조합 페디그리 서버의 signerInfo에 따라 issuerAddress를 ContactType으로 작성하여 조합의 정보를 기록하고 수신한 사설 인증 페디그리의 사설 검증을 위한 repositoryUrl 주소를 기록한다. 조합의 페디그리 서버는 조합 내에서 전달된 사설 인증 페디그리를 receivedPedigree에 포함하고 개인키로 서명함으로써 조합원의 페디그리 서버에서 작성한 사설 인증 페디그리를 보증한다. receivedPedigree의 signerInfo 정보와 issuerAddress의 정보는 동일해야 하고 동일한 경우에만 페디그리 서버는 해당 사설 인증 페디그리가 유효하다고 판단해야 한다.

8.4 페디그리 서버 요구사항 4: 사설 인증 페디그리 인증

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 협동 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 인증해야 한다.

9 사설 인증 절차 요구사항

조합에서 전달된 사설 인증 페디그리를 수신한 조합 외부의 페디그리 서버는 사설 인증 페디그리의 검증을 위해 사설 인증 서버에 접근하여 페디그리 인증 절차를 진행할 수 있다. 본 단락에서는 협동조합 내에서 생성 및 갱신된 페디그리의 사설 인증 절차의 요구사항에 대하여 기술한다.



(그림 9-1) 도매업자에게 전달된 사설 인증 페디그리 예시

농축산 협동조합 외부의 페디그리 서버에서 그림 9-1의 페디그리를 수신하면 농축산 협동조합의 receivedPedigree 내 privateDocumentInfo를 인식하여 포함된 페디그리들의 서명에 대한 사설 인증 절차를 수행해야 한다. 이 사설 인증 절차는 다음의 요구사항을 만족하여야 한다.

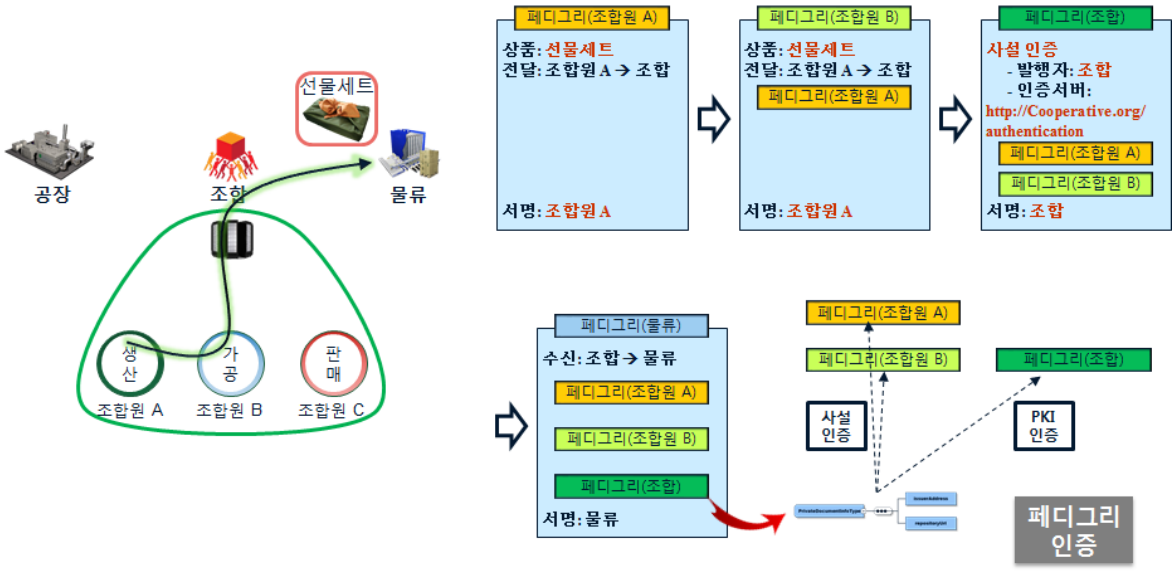
- privateDocumentInfo가 발견되면 issuerAddress의 정보가 receivedPedigree의 signerInfo와 동일한지 확인한다. 동일한 경우에만 인증 절차를 진행한다.
- repositoryUrl은 TLS 연결을 통해 접근해야 하고 member의 인증서를 응답받을 수 있어야 한다.
- repositoryUrl로 접근할 때는 파라미터로서 signerInfo와 signatureDate를 전송하

고, signerInfo 파라미터의 값은 사설 인증 대상 페디그리의 signerInfo 내 name 필드를 전송하고 signatureDate 파라미터의 값은 사설 인증 대상 페디그리의 signatureDate 필드의 값을 전송한다.

- 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 인증을 수행해야 한다.
- 사설 인증 대상 페디그리 내에 repackagedPedigree가 포함된 경우 previousPedigrees에 포함된 페디그리는 사설 인증 대상이다. issuerAddress와 비교하여 동일한 이름의 signerInfo를 가지는 페디그리가 발견될 때 까지 사설 인증을 수행해야 한다.

10 활용 예제

10.1 조합 내 생산품의 유통과 인증

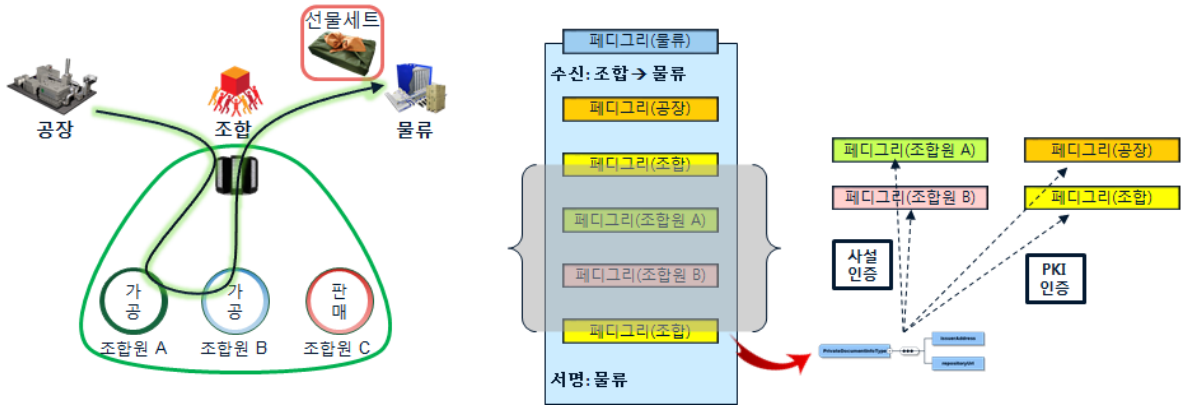


(그림 10-1) 사설 인증 필드에 의한 인증 과정

협동조합의 조합원으로부터 생산된 제품이 조합 외부로 판매되는 경우 사설 인증 페디그리의 유통단계별 생성 과정은 그림 10-1과 같다. 유통 과정에서 페디그리는 각각의 유통 단계에서 중첩/생성되어 그림 10-1과 같은 형태를 가지며 특별히 조합을 거쳐 외부로 이동할 때 조합에 의해 사설 인증을 위한 정보가 저장된다.
사설 인증 정보는 사설 인증을 수행할 주체(조합)의 정보가 포함되며 사설 인증을 위해 접근할 사설 인증 서버의 주소가 명시된다. 페디그리의 검증을 수행하고자 하는 주체는 누구나 PKI와 사설 인증 서버를 접근하여 페디그리 정보 및 서명에 대한 검증을 수행할 수 있으며 그림 10-1의 경우 사설 인증 정보를 이용하여 조합원 A와 조합원 B에 대한 검증은 사설 인증 서버를 통하여, 조합의 검증은 PKI를 통하여 이루어진다.

10.2 조합 내 가공품의 유통과 인증

협동조합 외부에서 생산된 제품이 조합 내의 조합원에 의해 가공되어 다시 조합 외부로 판매되는 경우 사설 인증 페디그리의 최종 모습은 그림 10-2과 같다. 사설 인증 페디그리는 각각의 유통 단계에서 중첩/생성되며 유통 과정에서 이동한 경로 순서대로 각 주체에서 생성된 페디그리 정보를 가지고 있다.



(그림 10-2) 사설 인증 페디그리의 사설 인증 범위

사설 인증 정보는 기본적으로 사설 인증을 제공하는 주체(조합)의 정보와 사설 인증을 위해 접근할 사설 인증 서버의 주소가 명시된다. 이 정보는 다른 페디그리의 signerInfo 정보와 결합되어 사설 인증을 수행할 사설 인증 페디그리의 범위를 한정하는데 이용 가능하다. 그림 10-2에서 최종 생성된 페디그리는 실제로 어떤 제품이 조합을 거쳐 조합 내부로 이동했고 또한 조합을 통해 조합 외부로 이동한 정보를 가진다. 즉, 어느 한 페디그리에서 사설 인증 정보가 나타나면 해당 페디그리에 포함된 모든 페디그리는 조합의 정보가 signerInfo에 나타날 때 까지 모든 페디그리를 사설 인증한다. 이 범위는 그림 10-2에서 나타난 바와 같이 조합원들이 작성한 페디그리를 의미한다. 따라서 최종 사설 인증할 사설 인증 페디그리의 정보는 그림 10-2과 같이 한정될 수 있다. 여러 개의 조합을 거치는 경우 다수의 사설 인증이 나타날 수 있으며 이때의 사설 인증은 각각의 사설 인증 서버를 통해서 인증 가능하다.

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

Ⅰ-1.1 지식재산권 확약서(1)

해당사항 없음

Ⅰ-1.2 지식재산권 확약서(2)

해당사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

해당사항 없음

Ⅰ-2.2 시험표준 제정 현황

해당사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

해당사항 없음

Ⅰ-3.1

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] EPCglobal, Pedigree Ratified Standard, version 1.0, January 2007.

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	xxxx.xx.xx	제정 TTAx.xx-xx.xxxx	-	스마트농업 프로젝트그룹 (PG426)