인증서와 전자서명을 이용하는 QR코드 기반 안심택배서비스

권현주*, 신세영*, 유현진*, 이병천**

*중부대학교 정보보호학과 (대학생), **중부대학교 정보보호학과 (교수)

QR code-based secure delivery service using certificates and digital signatures

Hyeonju Kwon*, Seyeong Shin*, Hyeonjin Yoo*, Byoungcheon Lee**

Department of Information Security, Joongbu University

요 약

개인정보의 유통을 기반으로 하는 금융, 인터넷, 전자상거래 등 다양한 산업의 발전에 따라 개인정보 보호의 중요성이 증가하고 있다. 그럼에도 불구하고 택배 운송장에 노출된 개인정보로 인한 범죄가 지속되고 있어 개인정보보호의 필요성이 제기되고 있다. 그 대책의 일환으로 가상번호 시스템과 코팅 처리기술 등을 이용해 개인정보를 보호하려고 하는 시도가 있는데 이들 방법은 개인정보를 부분적으로만 보호할 수 있다는 단점이 존재한다. 본 논문에서는 택배 운송장을 QR코드로 대체하고 인증서와 전자서명을 활용하여 인가된 택배기사, 구매자에게만 개인정보에 접근이 가능하도록 안심택배서비스를 설계하였다. 제안된 방식에서는 택배기사 및 구매자가 인증서가 구비된 안심택배앱을 이용한다. 택배기사는 QR코드 스캔 기능을 이용하여 택배물품을 배정받고 안심택배앱을 택배업무에 활용할 수 있고 인가된 구매자는 QR코드 스캔으로 택배물품의 내용을 확인할 수 있다. 본 연구에서는 QR코드를 이용하여 개인정보 노출의 위험을 줄일 수 있는 방향으로 업무 프로세스를 개선하는 가능성을 모색해 보고자 한다.

I. 서론

한국 통합물류협회에 따르면 국내의 택배 산업은 코로나바이러스 사태로 인해 2020년 국내 총 택배 물량이 33억7373만개로 집계되었으며 27억8980만개였던 전년 대비 20.9%의 증가율을 보였다. 택배 산업은 크게 확장되는 반면에 운송장에는 고객의 개인정보가 그대로 노출되어 있어 사회공학적 공격과 피싱 등 개인정보를 이용한 범죄들이 발생하고 있다. 2021년 3월에 발생한 노원 세 모녀 살인 사건은 택배 운송장에 그대로 노출되어 있는 개인정보가 이용된 것으로 알려져 택배 운송장에서 노출되는 개인정보에 대한 우려의 목소리가 점차 커지고 있다.

본 연구에서는 이러한 범죄를 예방하기 위해 전통적인 택배 운송장을 QR코드로 대체하여 개인정보를 보호하면서도 택배업무를 효율적으로 수행할 수 있도록 하는 안심택배서비스를 설계하였다. 택배기사는 서버로부터 발급받은 인증서를 통해 로그인을 해야만 서비스용 안심택배앱을 이용하여 택배서비스를 제공할 수 있다. 고객은 고객용 안심택배앱을 설치하고 사용자 등록 후 인증서를 발급받고 인증서를 이용하여 로그인한 후 서비스를 이용할 수 있다. 이처럼 인증기술을 통해 인가된 사용자만 개인정보에 접근이 가능하도록 하여 개인정보를 보호할 수 있다.

구체적으로는 택배물품에 운송장번호를 인쇄하고 이것이 포함된 QR코드를 부착한다. 택배기사는 서비스용 안심택배앱으로 QR코드를 스캔하여 해당물품을 배정받을 수 있고 배달주소는 서버에서 보내주게 되며 앱의 지도상에 주소가 표시된다. 인가되지 않은 타인이 QR코드를 스캔하면 서버에서 정보를 제공하지 않는다. 배달이 완료된 후 구매자는 QR코드를 스캔하여 자신의 물품이 맞는지 확인할 수 있다.

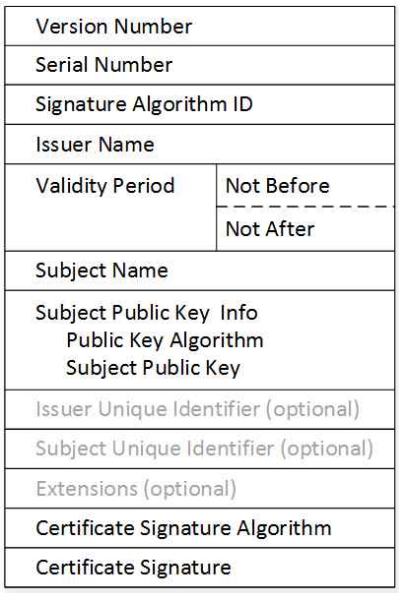
이후의 논문은 다음과 같이 구성되어 있다. 2장은 기반기술인 인증서와 QR코드 기술에 대

해 간단히 설명한다. 3장에서는 상세한 시스템 설계를 제시하고 4장에서는 이 시스템의 보안성을 분석한다. 5장에서는 결론으로 마무리한다.

II. 관련 연구

2.1 인증서

X.509 인증서는 개인정보와 공개키를 결합하여 인증기관이 서명한 문서로서 해당 공개키를 해당 개인이 소유하고 있음을 증명하며 인증서를 이용한 전자서명은 거래의 부인방지 기능을 제공한다. 공개키기반구조(PKI)는 X.509 인증서의 신뢰를 제공한다. 최근 우리나라에서는 공인인증서 제도의 폐지에 따라 사설인증서가 다양하게 사용될 것으로 예상된다.



〈그림 1. X.509 인증서의 구조〉

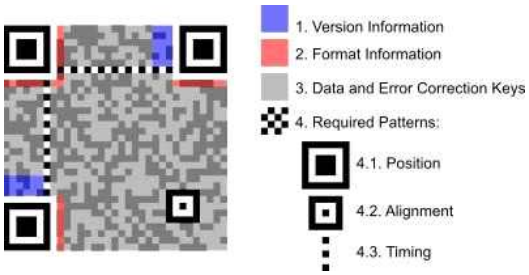
2.2 QR코드

QR코드란 흑백 격자무늬 형태로 정보를 나타내는 매트릭스 형식의 이차원 코드로 2000년에 ISO/IEC 18004 국제 규격으로 인정되었다[1].

QR코드는 바코드의 수십 배 내지 수백 배 정도의 대용량 정보 수납이 가능하고, 모양 또는 기능에 따라 Micro QR코드, iQR코드, Frame QR코드, SQRC로 분류된다. QR코드는 오류 복원 기능을 통하여 오염 및 손상이 있더라도 최대 30%까지 복원이 가능하고, QR코드 내부의 3개의 네모 격자(Position Required Patterns)로 어느 방향에서든 인식이 가능하다.

[표 1] QR코드 사양

코드크기	21×21cell ~ 177×177cell (4cell/변 씩 증가)	
정보 종류 및 정보량	숫자	최대 7,089문자
	영숫자	최대 4,296문자
	8bit byte	최대 2,953문자
	영자	최대 1,817문자
오류복원 능력 (데이터 복원기능)	Level L	약 7% 복원가능
	Level M	약 15% 복원가능
	Level Q	약 25% 복원가능
	Level H	약 30% 복원가능
코드 연결 기능	최대 16분할 (좁고 긴 공간에 인쇄)	



〈그림 2. QR코드의 구성〉

QR코드는 특정 정보를 카메라를 가진 다른 컴퓨터로 광학적으로 전달할 수 있는 매우 유용한 수단이다. 웹사이트 주소 등 고정된 정보를 전달하는 수단 뿐만 아니라 제로페이 등의 지불수단, 네이버의 QR코드 로그인 등의 로그인 수단, 코로나 출입내역 관리 수단 등으로 최근 용도가 대폭 확대되고 있다.

QR코드의 사용이 증가하면서 그에 따른 범죄 또한 증가하고 있다. QR+피싱의 합성어로 '큐싱'으로 불리는 위변조 공격이 증가하고 있다.

III. 시스템 설계

QR코드는 인터넷 통신을 사용하지 않고 근접한 사용자에게 광학적 방식으로 정보를 직접 전달하는 방식으로 고급 카메라 기능을 가진 휴대폰의 확산으로 인해 사용량이 크게 확대되고 있다. 전통적인 택배서비스는 바코드리더 등의 부가적인 장비를 사용하거나 인쇄된 운송장 정보에 의존하는 방식이었다. 본 연구는 택배기

사를 포함하여 누구나 사용하고 있는 휴대폰에 설치되는 앱을 이용하여 개인정보보호 기능을 제공하면서도 효율적인 물류서비스를 구성할 수 있는지 검토해 보려는 시도이다.

3.1 구현 환경

본 논문에서 개발하는 서비스 및 어플리케이션은 백엔드로 node.js 및 express를, 모바일 프런트엔드로는 Ionic과 Angular 프레임워크를 사용한다. Ionic 프레임워크는 데스크톱 및 프로그레시브 웹 앱을 개발하기 위한 도구와 서비스를 제공하여 iOS, Android와 같은 다양한 모바일 플랫폼에서도 빌드하고 배포가 가능하다는 장점이 있다. 서버와 데이터베이스는 구글의 Firebase를 사용하였다. 구현환경을 아래 [표 2]로 정리하였다.

[표 2] 구현 환경

백엔드	node.js, express
프런트엔드	Angular
모바일	Ionic
서버	Firebase
데이터베이스(DB)	
스마트폰 OS	IOS, Android

3.2 참여자별 기능

기존의 전통적인 운송장에는 고객 정보, 판매자 정보, 상품명, 박스수량, 운임요금, 정산구분, 특이사항, 주문번호, 운송장번호, 접수일자, 물류센터용, 배송정보, 배송캠프, 배송기사의 정보, 택배 회사 전화번호 등 많은 개인정보가 포함되어 있다. 이들 정보는 택배기사에게 필요한 정보도 있지만 이렇게 누구나 볼 수 있는 형태로 프린트되어 부착됨으로써 과도한 개인정보가 노출되고 있다. 여기에서는 기존의 전통적인 운송장을 최소한의 정보만을 포함하는 QR코드로 대체하려고 한다.

QR코드는 누구나 접근할 수 있는 특징을 가지고 있기 때문에 노출되어도 상관없는 최소한의 정보만을 넣어야 한다. 택배사의 서비스 시나리오에 따라 달라지겠지만 여기에서는 QR코드에 송장번호만을 포함하는 것으로 모델을 간략화하였다. 이 송장번호를 이용하여 인가된 택배기사 및 구매자는 서버에서 제공하는 개인정보 및 물품정보를 얻을 수 있다. 제안하는 서비스 및 앱 설계에서는 서버, 택배기사, 구매자의 3가지 참여자가 존재한다.

3.2.1 서버

서버는 판매업체에서 제공한 송장번호, 구매자정보 및 물품정보 등을 데이터베이스에 저장한 뒤 택배기사 또는 접근자가 정보를 요청하면 접근자의 신분 확인 절차를 거쳐 정보를 제공해준다. 확인절차에는 서버에서 발급해준 인증서가 필요하다.

택배기사 및 사용자가 인증서 발급을 요청하면 서버는 택배기사 및 사용자의 인증정보를 바탕으로 인증서를 발급해주고 각각의 계정에 인증서를 저장한다. 택배기사 또는 접근자가 정보를 요구하는 경우 전자서명을 포함해서 요청해야 하는데 인증서를 이용하여 인가된 사용자인지, 해당 송장번호의 정보에 접근권한이 있는지 확인한 후 정보를 제공한다.

3.2.2 택배기사

택배기사는 서비스용 안심택배 앱을 휴대폰에 설치하고 로그인한 후 서버에 인증서 발급을 요청한다. 서버는 소속 택배회사의 확인을 거쳐 인증서를 발급하고 택배기사의 계정에 인증서를 저장한다. 택배기사는 인증서를 이용하여 서비스에 로그인을 할 수 있다.

택배물품을 배정받기 위해서 택배기사는 QR스캐너 기능을 사용하여 택배 물품에 부착된 QR코드를 스캔한다. QR코드를 통해 송장번호가 택배기사의 앱으로 전달되는데 이때 앱은 전자서명이 포함된 물품배정요청 메시지를 서버로 전송한다. 서버는 전자서명 검증 후 택배기사의 정보를 데이터베이스에 저장함으로써 해당물품에 대해 택배기사를 배정해주고 배달업무에 필요한 배송지정보를 택배기사에게 전송한다.

택배기사는 자신에게 배당된 물품의 운송장번호와 그 배송지 정보를 휴대폰의 지도에서 확인할 수 있어서 택배업무에 유용하게 사용하게 된다.

택배의 배송이 완료되면 택배기사는 전자서명이 포함된 택배완료 메시지를 서버에 전송하고 서버는 전자서명 검증 후 택배완료 처리하며 구매자에게 택배완료 메시지를 전송하게 된다.

3.2.3 구매자

구매자는 고객용 안심택배 앱을 설치하고 회원가입을 진행한 뒤 로그인한다. 로그인한 구매자는 서버에 인증서 발급을 요청하여 발급받을 수 있으며 서버는 해당 구매자의 계정에 인증서를 저장한다.

구매자가 물품을 구매하면 운송장번호, 물품정보, 구매자정보가 서버의 데이터베이스에 저장되는데 구매자는 자신이 구매한 운송장번호에 대해 정보를 요청할 권한이 발생하며 배송현황을 파악할 수 있다.

택배가 완료된 경우 해당 패키지에는 운송장번호가 포함된 QR코드만 인쇄되어 있다. 구매자는 고객용 안심택배앱을 이용하여 QR코드를 스캔하면 물품정보확인요청이 서버에 전송되며 서버는 구매자의 권한을 확인 후 해당 물품의 자세한 정보를 전송해준다.

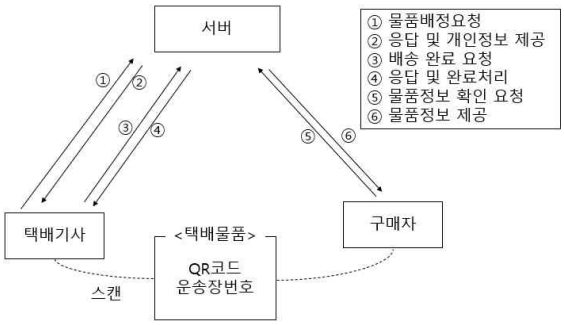
3.3 택배 배송 서비스 단계

택배기사는 서비스용 안전택배앱을 설치하여 로그인하고 서버로부터 인증서를 발급받는다. 인증서와 개인키는 앱에 저장되고 서버는 택배기사의 계정에 인증서를 저장한다. 로그인시 및 업무시 개인키를 이용한 전자서명이 이용된다.

구매자는 고객용 안전택배앱을 설치하여 로그인하고 서버로부터 인증서를 발급받는다. 인증서와 개인키는 앱에 저장되고 서버는 고객의 계정에 인증서를 저장한다. 로그인시 및 물품확인시 개인키를 이용한 전자서명이 이용된다.

1) 택배기사의 물품 배정

택배기사는 자신이 담당하는 구역의 물품을 수령하고 물품배정 요청을 위해 서비스용 안심택배앱의 QR 스캔 기능을 이용하여 물품에 인쇄된 QR코드를 스캔한다. 안심택배앱은 <택배기사 정보, 운송장번호, 요청 시간>을 택배기사의 개인키로 서명하여 서버에 전송한다. 서버는



<그림 3 시스템 단계별 구조>

해당 정보를 검증한 후 데이터베이스에 해당 운송장번호에 배정된 택배기사의 정보를 추가한다. 그리고 배정된 물품에 대한 배송지정보를 택배기사에게 전송한다.

2) 택배기사의 배송 서비스

서비스용 안심택배앱에서 택배기사는 자신에게 배정된 물품들의 운송장번호 및 배송지정보를 지도위에서 확인할 수 있다. 서버는 효율적인 이동동선과 배송할 물품의 순서를 알아보기 쉽게 표시해줄 수 있다.

3) 배송 완료

택배기사는 배송 완료 후 해당 운송장번호에 대한 배송 완료 버튼을 누른다. 서비스용 안심택배앱은 <택배기사정보, 운송장번호, 배달완료시간>을 택배기사의 개인키로 서명한 정보를 서버로 전송한다. 필요시 택배기사가 카메라를 이용하여 배송 완료된 물품의 사진을 찍어서 보내는 기능을 구현할 수도 있다.

서버는 택배기사의 전자서명을 검증 후 배송완료 처리한다. 이때 서버는 고객에게 배송완료 메시지를 보내게 된다.

4) 구매자의 물품 정보 확인 요청

구매자가 받은 택배 패키지에는 운송장번호가 포함된 QR코드만이 인쇄되어 있다. 구매한 물품의 자세한 정보를 확인하기 위해서 구매자는 고객용 안심택배앱을 이용하여 해당 QR코드를 스캔할 수 있으며 이때 <구매자정보, 운송장번호, 현재시간>에 대해 구매자가 서명한 정보

를 서버에 전송한다. 서버는 구매자가 해당 운송장번호의 구매자인지 확인한 후 물품의 상세정보를 제공한다.

IV. 분석

2015년 김무환 등이 제시한 QR코드를 이용하여 프라이버시 보호 기능을 제공하는 택배서비스는 OTP 방식의 일회용 암호키를 이용하여 암호화된 QR코드를 생성하는 방식이었다[3,4]. 이러한 방식은 택배회사, 택배기사, 구매자 사이에 키를 공유하는 관리방식이 복잡하여 운영이 어렵고, 이러한 방식을 운영 가능하게 만들기 위해서는 많은 취약점이 발생할 것으로 예상된다. 반면 본 논문에서 제시하는 방식은 기본적으로 모든 개인정보를 서버가 관리하고 정당한 택배기사 및 구매자가 요청하는 경우에만 정보를 제공하는 방식이다. 로그인과 업무처리 등에 전자서명을 부가하여 요청하게 되며 서버는 보관하고 있는 인증서를 이용하여 서명을 검증하는 방식으로 안전하면서도 서비스 운영이 매우 편리하다.

공격자는 QR코드의 취약점을 이용하여 다음과 같은 공격행동을 취할 수 있을 것이다[2].

1) 타인의 QR코드 스캔

공격자가 타인의 개인정보획득을 목적으로 타인의 택배물품의 QR코드를 스캔할 수 있다. QR코드에는 판매자가 생성하는 일회용 운송장번호만 표시되고 상세한 개인정보는 서버로부터 받아와야 하는데 서버는 접근요청자의 신원을 확인하고 서명을 검증한 후 권한이 있는 경우에만 정보를 제공하므로 개인의 정보를 보호할 수 있다.

2) QR코드의 위변조

택배운송장에 부착되는 QR코드는 인쇄된 QR코드이기 때문에 공격자가 위조된 QR코드를 생성하여 기존 QR코드 위에 덧붙일 수 있다. 이런 공격을 방지하기 위해서는 고급 인쇄기술 및 코팅처리기술 등 물리적인 위조방지 기술을 활용할 수 있을 것이다. QR코드를 스캔하는 택배기사 및 구매자는 QR코드가 혹시 변조된 것이 아닌지 확인해야 한다.

QR코드의 위변조를 막기 위해 암호학적 대책을 사용할 수 있다. 택배회사가 전자서명이 포함된 QR코드를 생성하여 부착할 수 있는데[2] 이 경우 택배기사 및 구매자가 전자서명을 검증하여 QR코드의 유효성을 검증할 수 있게 된다.

V. 결론

언커넥티드 시대에 발맞춰 택배, 배달 서비스의 사용률이 크게 증가하고 있으며 그에 따라 개인정보 노출에 의한 범죄 또한 증가하는 추세이다.

본 논문에서는 많은 개인정보가 그대로 노출되어 있는 전통적인 운송장 대신에 판매자가 부여하는 운송장번호만을 포함하는 QR코드를 사용하여 택배서비스를 재구성해보고자 하였다. 이러한 안심택배서비스는 물품정보 및 배송정보 등 상세 개인정보를 서버가 관리하며 요청자의 신원과 권한을 확인한 후 제공하게 되므로 개인정보호 기능이 크게 향상된 것으로 생각할 수 있다. 현재 이러한 설계를 바탕으로 서비스 구현을 진행중이다.

[참고문헌]

[1] DENSO WAVE, the Inventor of QR Code, QR코드의 사양 및 특징, https://www.qrcode.com/ko/

[2] 양형규, QR 코드의 보안 취약점과 대응 방안 연구, 한국인터넷방송통신학회 논문지, v.12 no.1, pp. 83-89, 2012년.

[3] 김무환, 신용태, 택배 서비스 프라이버시 보호를 위한 암호화 기반의 QR코드 택배 운송장과 인식 어플리케이션 설계, 한국IT서비스학회 2015추계학술대회 논문집, 392 - 395, 2015.

[4] 김무환, 택배서비스 개인정보보호를 위한 QR코드 운송장과 인식 프로토타입 구현, 숭실대학교 석사학위논문, 2015년 12월.