情 報 保 護 學 會 誌
第23卷 第3號, 2013. 6

OTP 기반 인증기술 국제 표준화 동향

김 근 옥*, 심 희 원**

요 약

최근, 피싱 파밍 등 전자거래 환경의 보안위협의 크게 증가하면서 안전한 전자거래를 위한 다양한 인증기술에 대한 논의가 활발히 진행되고 있다. 본 논문에서는 이와 관련하여 ITU-T SG17 국제표준화기구에서 추진하는 OTP 기반 부인방지에 대한 표준안을 분석하고, 해당 프레임워크의 실제 전자거래 환경에 적용하기 위한 방안을 분석한다. 기존 전자거래 환경에서는 전자거래에 대한 부인방지 기능을 제공할 수 있는 기술로 공개키 기반의 전자서명이 주로 사용되었는데, 해당 표준안은 대칭키 기반의 일회용패스워드(OTP) 기술을 이용해서 부인방지 기능을 제공할 수 있는 새로운 방법을 제시하고 있다.

OTP 부인방지 프레임워크는 사용자와 서비스제공자가 OTP 생성키를 이용해서 거래정보와 연계된 부인방지토큰 요청 메시지를 생성하고, 제3의 신뢰기관인 TTP를 통해 부인방지토큰을 생성 및 검증한다. 해당 프레임워크에서는 부인방지 서비스를 제공하기위한 4가지 서비스 모델을 제시하고 있어서, 전자거래환경에 맞는 서비스 모델을 선택적으로 적용이 가능하다.

Ⅰ. 서 론

최근, 피싱 파밍 등 전자거래 환경의 보안위협의 크게 증가하면서 안전한 전자거래를 위한 다양한 인증기술에 대한 논의가 활발히 진행되고 있고, 전세계적으로는 전자거래의 안전성 확보를 위해 OTP의 사용이 꾸준히 증가하고 있는 추세이다. Smart Insight의 보고서[1]에 따르면, 2015년 전 세계적으로 OTP 이용자가 10억명을 초과할 것으로 예상하고 있다. 또한 스마트폰의 급속한 보급으로 인해 국내 모바일뱅킹 가입자수는 이미 4000만명을 돌파했다[2]. 이제 국내에서도 스마트폰, IPTV 등 다양한 전자거래 환경에서 보다 안전하면서 사용자 편의성을 높인 인증기술에 대한 요구가 증가하고 있다. 최근 이를 위한 방안으로, 전자거래 환경에서 널리 보급되어있는 OTP를 활용한 새로운 인증기술에 대한 연구가 지속적으로 진행되었다.

Ⅱ. OTP 부인방지 표준안 개요

OTP 부인방지 표준안[3]은 2011년 4월 ITU-T Q.7/SG17 (어플리케이션 보안) 그룹에서 표준화 작업을 착수하여, 이번 2013년 4월 국제회의에서 최종 국제표준 채택을 위한 준비과정(consent)에 승인되었으며, 4주간 각 국가의견을 수렴하여, 반대하는 국가가 없으면 2013년 6월중에 최종 등록될 예정이다.

기존 전자거래 환경에서는 전자거래에 대한 부인방지 기능을 제공할 수 있는 기술은 공개키 기반의 전자서명이 유일한 기술이었는데, 이번 OTP 부인방지 표준안을 통해 대칭키 기반의 기술을 이용해서도 부인방지 기능을 제공할 수 있는 새로운 방법을 제시하였다.

OTP 부인방지 표준안은 거래 객체간의 신뢰성을 제공하기 위해 일회용비밀번호 기반의 부인방지 서비스를 제공하기 위한 보안 요구사항 뿐만 아니라, 부인방지 토큰을 생성하기 위한 메커니즘을 설명하고 있다. TTP는 부인방지 토큰을 생성 및 검증을 수행한다. 특히, 본 표준안에서는 일회용비밀번호 기반의 4가지 부인방지 서

본 연구는 미래창조과학부의 지원을 받는 방송통신표준기술력향상사업의 연구결과로 수행되었음
* 금융보안연구원 인증서비스 본부 인증기술팀 (kko@fsa.or.kr)
** 금융보안연구원 인증서비스 본부 인증기술팀 (hwshim@fsa.or.kr)

비스 모델을 정의하고 있어, 다양한 전자거래 환경에 적용이 가능하다.

Ⅲ. OTP 기반 부인방지 프레임워크

OTP 기반 부인방지 프레임워크는 OTP를 이용해서 거래데이터의 송·수신 사실에 대해 부인하는 것을 방지하기 위한 프레임워크 이다. OTP 기반 부인방지 프레임워크는 거래의 신뢰성을 보장하기 위해 inline TTP가 반드시 필요하며, 사용자와 TTP가 나눠가진 OTP 생성키를 이용해서 한번만 사용할 수 있는 부인방지토큰요청 메시지를 생성하고, 신뢰할 수 있는 제3의 기관인 TTP가 부인방지 토큰을 생성 및 검증한다.

OTP 기반 부인방지 프레임워크는 거래데이터의 송신사실에 대해 부인을 방지하는 송신부인방지(NRO)와 거래데이터의 수신사실에 대해 부인을 방지하는 수신부인방지(NRD)를 제공한다.

3.1 부인방지 토큰의 종류

전자거래에서 사용되는 부인방지 토큰은 크게 송신부인방지토큰(NROT, Non-Repudiation of Origin Token)과 수신 부인방지토큰(NRDT, Non-repudiation of Delivery Token)으로 이루어진다. 송신부인방지토큰(NROT)은 OTP 사용자가 거래 데이터를 송신한 사실에 대해 부인을 방지하기 위해 필요한 부인방지토큰이며, 수신부인방지토큰(NRDT)은 서비스제공자가 거래데이터를 수신한 사실에 대해 부인하는 것을 방지하기 위한 부인방지 토큰이다.

그렇기 때문에 송신부인방지토큰(NROT)은 서비스제공자가 보관하고, 분쟁 발생 시 송신부인방지토큰(NROT)을 검증하여 거래 데이터에 대해 송신자의 행위를 증명할 수 있다. 또한, 수신부인방지토큰(NRDT)은 OTP 사용자가 보관하고, 분쟁 발생 시 수신부인방지토큰(NRDT)을 검증하여 거래 데이터에 대해 수신자의 행위를 증명할 수 있다.

3.2 OTP 기반 부인방지 프레임워크 객체

OTP 기반의 부인방지프레임워크는 OTP 사용자, 서비스 제공자의 제3의 신뢰기관인 TTP로 구성된다.

OTP 사용자는 거래데이터의 주체로 OTP 방식을 이용해서 거래데이터에 대한 송신부인방지토큰(NROT)를 TTP에 요청하고, TTP가 생성한 부인방지토큰을 서비스제공자에게 전달한다. 또한 OTP 사용자는 수신부인방지토큰(NRDT)를 관리하고, 서비스제공자가 거래데이터의 수신사실에 대해 부인할 경우 해당 토큰을 검증함으로써 분쟁을 해결할 수 있다.

서비스 제공자는 거래데이터를 수신하는 주체로, OTP 사용자로부터 거래데이터를 수신하면, 수신부인방지토큰(NRDT)를 TTP에게 요청하고, TTP가 생성한 부인방지토큰을 OTP 사용자에게 전달한다. 또한 서비스제공자는 송신부인방지토큰(NROT)를 관리하고, OTP 사용자가 거래데이터의 송신사실에 대해 부인할 경우 해당 토큰을 검증함으로써 분쟁을 해결할 수 있다.

TTP는 송·수신부인방지토큰을 생성 및 검증하는 주체로, OTP 기반 부인방지 프레임워크에서는 inline TTP를 기본 전제로 한다.

3.3 OTP 기반 부인방지 절차

부인방지는 거래데이터의 송·수신자가 거래사실에 대해 부인하는 것을 방지하는 것을 의미한다. OTP 기반 부인방지는 객체가 거래데이터를 포함한 OTP 기반의 부인방지토큰 요청 메시지를 생성하여 TTP에 부인방지토큰 생성을 요청하면, TTP는 요청 메시지를 검증한 후, 부인방지토큰을 생성하여 전달하고, 부인방지토큰의 검증 요청에 대해서도 요청메시지 검증 후 부인방지토큰을 검증하여 결과를 전달한다.

3.3.1 부인방지토큰 요청 메시지 및 부인방지토큰 생성

a) 거래데이터를 포함한 메시지 z'를 구성하고, 미리 발급받은 OTP 키를 이용해서 아래와 같이 OTP 기반의 부인방지토큰 요청메시지 SEVO를 생성해서 TTP에게 부인방지토큰을 요청한다.

단, z는 객체의 식별정보, 메시지 생성 및 송수신 시각정보, 거래데이터 정보 등 인증을 위한 정보로 구성되며, z'는 z에서 시간 필드가 비워진 형태를 의미한다.

- $SEVO_X(z') = z' || OTP_X(z')$
- $OTP_X(z')$ = *OTP generation function (X, Sync data, [Token activation data]), where Sync data*

= {time and/or event counter and/or challenge and/or z}; [] optional input

b) 객체로부터 전달받은 부인방지토큰 요청메시지 SEVO를 검증 한 후, 유효하면 z'에 시간정보를 채워넣고, TTP의 키를 이용해서 부인방지토큰(NRT)을 생성한다.

- *NRT = text || z || mac*

text : 추가하고자 하는 메시지,
z : 시간정보가 포함된 메시지,
mac = $MAC_{ttp}(z)$

3.3.2 부인방지토큰 전달

TTP는 생성한 부인방지토큰을 OTP키를 이용해서 아래와 같이 SEVO를 생성하여 전달한다.

- *$SEVO_X(NRT) = z' || OTP_X(NRT)$*
- *$OTP_X(NRT)$ = OTP generation function (X, Sync data, [Token activation data]), where Sync data = {time and/or event counter and/or challenge and/or z}; [] optional input*

3.3.3 부인방지토큰 검증

부인방지토큰의 검증은 TTP를 통해서 할 수 있다. 부인방지토큰을 검증받고자 하는 객체는 부인방지토큰을 OTP키를 이용해서 아래와 같이 SEVO를 생성하여 TTP에 전달한다.

- *$SEVO_X(NRT) = z' || OTP_X(NRT)$*
- *$OTP_X(NRT)$ = OTP generation function (X, Sync data, [Token activation data]), where Sync data = {time and/or event counter and/or challenge and/or z}; [] optional input*

TTP는 전달받은 SEVO를 먼저 검증한 후, 유효하면 부인방지토큰에 대한 검증을 수행한다.

- *NRT = text || z || mac*

전달받은 NRT에서 z를 추출하고, *mac = MACttp(z)* 값을 생성하여 전달받은 mac 값과 비교하여 토큰을 검증한다.

Ⅳ. OTP 기반 부인방지 서비스 모델

OTP 기반 부인방지 서비스 모델은 제3의 신뢰기관인 TTP와 각 객체 사이에 부인방지 토큰을 전달하는 통신방법에 따라 4가지로 분류한다.

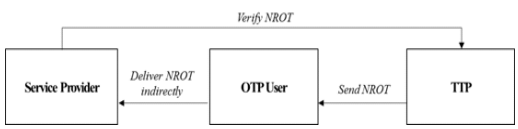
4.1 통신방법에 따른 부인방지 서비스 분류

각 객체가 제3의 신뢰기관인 TTP로부터 부인방지 토큰을 받는 방식은 크게 4가지가 있다. 서비스제공자에게 필요한 송신부인방지토큰(NROT)를 TTP로부터 직접 받는지, OTP 사용자를 통해 전달받았는지에 따라 direct NROT와 indirect NROT로 나눠진다.

[그림 1]은 Direct NROT 통신방법을 나타내며 서비스제공자가 TTP로부터 송신부인방지토큰(NROT)을 직접전달 받기 때문에 송신부인방지토큰(NROT)에 대한 별도의 검증절차는 필요하지 않다.

〔그림 1〕 Direct NROT 통신방법

[그림 2]는 Indirect NROT 통신방법을 나타내며 서비스제공자가 OTP 사용자를 통해서 TTP가 생성한 송신부인방지토큰(NROT)를 전달받기 때문에, 전달받은 부인방지토큰에 대한 별도의 검증 절차는 필요하다.

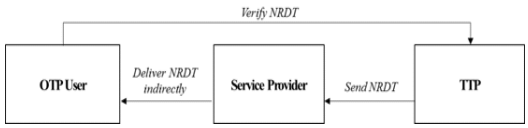


〔그림 2〕 Indirect NROT 통신방법

[그림 3]은 Direct NRDT 통신방법을 나타내며 OTP 사용자가 TTP로부터 수신부인방지토큰(NRDT)을 직접전달 받기 때문에 수신부인방지토큰(NRDT)에 대한 별도의 검증절차는 필요하지 않다.

〔그림 3〕 Direct NRDT 통신방법

[그림 4]는 Indirect NRDT 통신방법을 나타내며 OTP 사용자가 서비스제공자를 통해서 TTP가 생성한 수신부인방지토큰(NRDT)를 전달받기 때문에, 전달받은 부인방지토큰에 대한 별도의 검증 절차는 필요하다.

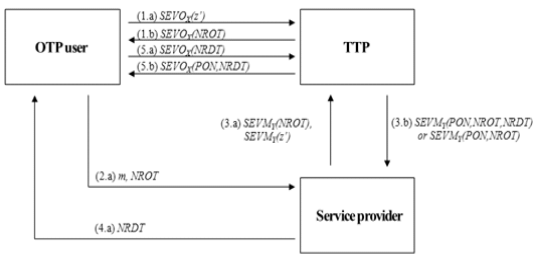


〔그림 4〕 Indirect NRDT 통신방법

4.2 OTP 부인방지 서비스 모델

OTP 부인방지는 4가지 모델로 구성된다. 해당 표준 안에서 제시하는 OTP 부인방지 서비스 모델은 ISO/IEC 13888-2[4]에서 제공하는 메커니즘을 준용하며, 본 논문에서는 가장 기본이 되는 'Indirect NROT and indirect NRDT' 서비스 모델을 설명한다.

해당 서비스 모델은 서비스제공자가 송신부인방지토큰(NROT)을 OTP 사용자를 통해 받고, OTP 사용자는 수신부인방지토큰(NRDT)을 서비스제공자를 통해 받는 형태의 서비스 모델이다.



〔그림 5〕 Indirect NROT and indirect NRDT 서비스 모델

(1) Transaction 1 – 송신부인방지토큰(NROT) 요청

(1.a) OTP 사용자는 OTP 기반의 부인방지토큰 요청 메시지 $SEVO_X(z')$를 생성하여 TTP에게 전달한다. 여기서 키 X 는 OTP 사용자의 키이며, z'는 3.1장에서 정의한 z에서 시간정보 Tg를 제외한 정보이다.

(1.b) TTP는 OTP 사용자로부터 전달받은 $SEVO_X(z')$를 검증한다. 만약 검증결과가 유효하면, TTP는 z'에 시간정보인 Tg를 채워 z를 만들고, 송신부인방지토큰(NROT)을 생성한다. TTP는 생성한 부인방지토큰에 대해 $SEVO_X(NROT)$를 생성해서 OTP 사용자에게 전달한다.

(2) Transaction 2 – 부인방지 서비스 요청

(2.a) OTP 사용자는 송신부인방지토큰과 거래 데이터를 서비스제공자에게 전달하고 부인방지 서비스를 요청한다.

(3) Transaction 3 – 송신부인방지토큰(NROT) 검증 및 수신부인방지(NRDT) 응답

(3.a) 서비스제공자는 거래데이터를 검증하고, $SEVM_Y(NROT)$와 $SEVM_Y(z')$를 생성한다. 키 Y는 서비스제공자의 키이다. 서비스제공자는 생성한 정보를 TTP에게 전달한다.

(3.b) TTP는 $SEVM_Y(NROT)$, $SEVM_Y(z')$, 송신부인방지(NROT)를 검증한다. 만약 유효하면, TTP는 z'에 시간정보인 Tg를 채워 z를 만들고, 수신부인방지토큰(NRDT)을 생성한다. 그리고, TTP는 $SEVM_Y(PON,NROT,NRDT)$를 생성해서 서비스 제공자에게 전달한다. 여기서 PON은 송신부인방지토큰(NROT)의 검증성공 결과값을 의미한다. 만약 송신부인방지(NROT)의 검증결과 유효하지 않으면, TTP는 PON에 검증실패 결과값을 설정하여 $SEVM_Y(PON,NROT)$를 서비스 제공자에게 전달한다.

(4) Transaction 4 – 수신부인방지토큰(NRDT) 전달

(4.a) 서비스제공자는 수신부인방지토큰(NRDT)를 OTP 사용자에게 전달한다.

(5) Transaction 5 – 수신부인방지토큰(NRDT) 검증

(5.a) 사용자는 OTP키를 이용해서 검증하고자 하는 수신부인방지토큰(NRDT)에 대한 $SEVO_X(NRDT)$를 생성하여 TTP에게 전달한다.

(5.b) TTP는 $SEVO_X(NRDT)$와 NRDT를 검증한다. 검증결과가 모두 유효하면, TTP는 PON에 검증성공 결과값을 설정 하고, $SEVO_X(PON,NRDT)$를 생성하여 OTP 사용자에게 전달한다. 만약 검증결과가 유효하지 않으면, TTP는 PON에 검증실패 결과값을 설정하고, $SEVO_X(PON,NRDT)$를 생성하여 OTP 사용자에게 전달한다.

V. 결 론

본 논문에서는 최근 ITU-T SG17에서 추진하고 있는 OTP 부인방지 프레임워크 표준안을 분석하였다. 최근 전자거래 환경이 다양화 되면서, 보안성과 편의성을 보장할 수 있는 새로운 인증기술에 대한 요구가 증가하고 있다. 해당 표준안의 OTP 부인방지 프레임워크는 전자거래환경에서 널리 사용되고 있는 OTP를 이용하여 부인방지를 제공할 수 있기 때문에 효과적이다.

OTP 부인방지 프레임워크는 스마트폰, IPTV 등 전자거래 환경이 다양화됨에 따라, 앞으로 더욱 다양한 전자거래 환경에 적용되어 송신자와 수신자간에 보다 신뢰할 수 있는 전자거래를 위한 방법으로 활용이 가능할 것으로 기대된다.

참고문헌

[1] *"Unconnected OTP Generator Market 2011"*, Smart Insight, February 2011.

[2] *"2013년 1/4분기 국내 인터넷뱅킹서비스 이용현황"*, 한국은행, May 2013.

[3] Recommendation ITU-T X.1156, "*An one time password based non-repudiation framework*", April 2013

[4] ISO/IEC 13888-2, *Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques*, 2009

〈著者紹介〉

김 근 옥 (Kim Keun Ok)
2004년 2월 : 성균관대학교 전자건기 컴퓨터공학과 석사
2011년 8월~현재 : 성균관대학교 전자건기 컴퓨터공학과 박사과정
2001년 3월~현재 : 금융보안연구원 인증기술팀 선임연구원
<관심분야> OTP, 암호이론, 정보보호

심 희 원 (Shim Hee Won)
정회원
2000년 2월 : 홍익대학교 전자계산기학과 석사
2011년 8월 : 전남대학교 정보보호학과 박사
2006년 12월~현재 : 금융보안연구원 인증기술팀 팀장
<관심분야> PKI, OTP, 네트워크 보안, 암호이론