情 報 保 護 學 會 誌
第22卷 第2號, 2012. 4

국내외 OTP 표준화 동향

송 성 현*, 김 근 옥**

요 약

OTP는 사용할 때마다 매번 새롭게 생성되는 일회용 비밀번호로, 전자적 해킹 위협의 증가로 강한 인증을 필요로 하는 산업계의 각 분야에서 활발하게 사용되고 있다. 국내에서는 OTP 기반 인증 기술이 금융, 전자정부, 게임, 포털사이트 등에 적용되었으며, 싱가포르는 국가 차원에서 OTP 발생기를 이용해 국가인증 프레임워크(NAF, National Authentication Framework)를 개발하여 서비스 준비 중에 있다. 이와 같이 OTP는 그 사용 범위가 날로 늘어나고 있으며, 이를 반영하듯 OTP 통합인증 프레임워크나 OTP기반 부인방지 기술 등의 표준화가 국내·외에서 활발하게 진행되고 있는 실정이다. 이에, 본 논문에서는 국내·외에서 제정되었거나 진행 중인 OTP 표준을 소개하고 대표적인 표준을 분석 및 정리하여 OTP 표준화 동향을 알아봄으로써 OTP 기술 및 표준의 개발에 참고가 될 수 있는 정보를 제공하고자 한다.

Ⅰ. 서 론

2012년 3월 국내 전자금융 이용자중 OTP 발생기를 발급받은 사람이 590만 명을 넘어섰다[1]. 현재 국내에서 OTP 기반 인증기술은 전자금융 뿐 아니라 전자정부, 게임, 포털사이트 등으로 그 적용범위가 점차 늘어나고 있는 추세이다. 또한, 스마트 환경에서 편리하게 사용가능한 USIM기반 모바일OTP 등의 기술개발로 향후 OTP 기반의 인증 서비스는 계속 늘어날 것으로 전망되고 있다.

유럽에는 EMV(Europay, Mastercard and Visa)에서 개발한 CAP(Chip Authentication Program)에 OTP 기술이 적용되어 활발히 사용되고 있고, 싱가포르에서는 국가 차원에서 OTP 발생기를 이용해 국가인증 프레임워크(NAF, National Authentication Framework)를 개발하여 서비스 준비 중에 있다.

이와 같이 OTP 기술이 활발하게 사용되고 있는 이유는 전자적 해킹 위협의 증가로 강한 인증을 필요로 하는 요구와 함께 국내·외에서 활발하게 진행되고 있는 표준화 작업이 기술 활성화의 밑바탕이 되고 있기 때문이다.

1995년 IETF에서 S/KEY 기반의 OTP 시스템 표준(RFC 2289)이 제정된 이래, 국내에서 금융보안연구원 주도하에 OTP 표준화가 이루어지고 있으며, 국외에서는 VeriSign등의 업체들이 참여하는 OATH(Open AuTHentication)와 RSA사를 주축으로 OTP 관련 표준화를 적극적으로 진행하고 있다.

따라서, 본 논문에서는 국내·외에서 진행되고 있는 표준화 동향에 대해서 알아보고자 한다.

본 논문은 다음과 같이 구성된다. 먼저 2장에서는 OTP 표준화 동향을 알아보고자 국내·외에서 제정되었거나 진행 중인 OTP 표준을 알아보고 이중 대표적인 OTP 표준에 대해서 설명한다. 이를 바탕으로 3장에서는 제시된 OTP 표준을 특성에 따라 분류하고 표준화 동향을 분석한다. 끝으로 4장에서는 본 논문의 결론을 맺는다.

Ⅱ. 표준화 동향

2.1 국내 OTP 표준화 동향

국내 OTP 표준은 TTA에서 금융보안연구원 주도로 진행되고 있다. 2009년 국내 전자금융 환경에 적용한 OTP 통합인증 프레임워크를 표준화한 이후로, OTP의 암호키 관리 기능에 대한 보안 요구사항을 정의한 "일

* 금융보안연구원 인증서비스본부 인증기술팀(decash@fsa.or.kr)
** 금융보안연구원 인증서비스본부 인증기술팀(kko@fsa.or.kr)

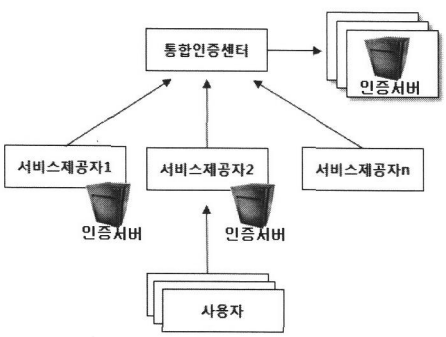
회용 패스워드(OTP) 암호키 관리 보안 요구사항"과 상호 연동성을 보장하는 응용 프로그램 인터페이스를 정의한 "OTP 검증서버를 위한 응용 프로그램 인터페이스" 표준 등을 제정하였다. 다음 [표 1]는 국내에서 제정된 OTP 표준을 나타낸다.

〔표 1〕 국내 OTP 표준

표준 제목	표준번호
일회용 패스워드(OTP) 암호키 관리 보안 요구사항	TTAK.KO-12.0100
일회용 패스워드(OTP) 인증서비스를 위한 보증 레벨	TTAK.KO-12.0120
일회용 패스워드(OTP) 통합인증 서비스 프레임워크	TTAK.KO-12.0128
일회용 패스워드(OTP) 키 컨테이너	TTAK.KO-12.0129
일회용 패스워드(OTP) 토큰 보안 요구사항	TTAK.KO-12.0130
일회용 패스워드(OTP) 검증서버를 위한 응용 프로그램 인터페이스	TTAK.KO-12.0132
일회용 패스워드(OTP) 기반 전자금융 거래검증 프로토콜	TTAK.KO-12.0167
일회용 패스워드(OTP) 기반 인증 서비스 관리 프로토콜	TTAK.KO-12.0168
일회용 패스워드(OTP) 검증 서버 보안요구사항	TTAK.KO-12.0169

2.1.1 일회용 패스워드(OTP) 통합인증 서비스 프레임워크(TTAK.KO-12.0128)

본 표준은[2] OTP 인증 서비스를 위한 OTP 통합인증 서비스 프레임워크의 모델 및 기능을 설명하고, 보안 고려사항을 정의하고 있으며, OTP 통합인증 서비스 모델과 서로 다른 도메인에 있는 통합인증센터간의 연동 모델을 정의하고 있다.



〔그림 1〕 OTP 통합인증서비스 모델

[그림 1]의 OTP 통합인증 서비스 모델은 다수의 사용자가 다수의 서비스 제공자들의 서비스를 받는 시나리오를 기반으로 구성된 것이며, 다수의 서비스제공자로부터 OTP 인증을 대행하는 통합인증센터가 구축되어있는 구조이다. 통합인증센터를 통해 서비스 제공자는 인증서버를 구축하지 않아도 OTP 서비스를 제공할 수 있으며, 사용자는 하나의 OTP생성기를 여러 서비스 제공자들에게 이용 등록하여 서비스를 이용할 수 있다.

OTP 통합인증서비스 모델은 모든 서비스제공자가 인증요청 등 모든 업무를 통합인증센터에 통하는 중앙집중식 서비스 모델로, 서비스의 안정성을 향상시키기 위해, 선택적으로 서비스제공자가 내부적으로 대체인증서버를 구축할 수 있다. 해당 표준에서는 서로 다른 도메인에 존재하는 통합인증센터간의 연동 모델도 소개하고 있다. 서비스하고자 하는 도메인의 서비스 요구사항과 보안정책을 분석하여 해당 도메인에 등록된 OTP 발생기를 허용할 경우 센터 등록 기능을 통해 연동 절차를 수행하는 방법을 정의하고 있다.

본 표준은 2011년 ITU-T X.1153 국제 표준으로도 제정된 상태이다.

2.1.2 일회용 패스워드(OTP) 암호키 관리 보안 요구사항 (TTAK.KO-12.0100)

2009년 제정된 본 표준[3]은 NIST의 SP 800-57 암호

〔표 2〕 암호키 관리 단계 및 기능

단계	기능	내용
준비단계	암호키 준비	키의 안전성을 고려하여 용도, 유효기간, 크기, 상태전이 등의 요구사항을 정의하는 기능
	암호키 생성	안전한 알고리즘 및 정책에 의해 키를 생성하는 기능
	암호키 배포	온라인 또는 오프라인으로 키를 배포하는 기능
운영단계	암호키 보호	외부로부터 안전하게 키를 보호하는 기능
	암호키 가용	키를 백업 및 복구하여 운영 시 가용성을 보장하는 기능
	암호키 변경	유효기간 만료로 키를 갱신하거나, 키가 노출되어 다른 키로 대체하는 기능
정지단계	암호키 정지	키의 노출이 의심되는 경우 즉시 사용정지 하는 기능
	암호키 폐기	키를 복구 불가능한 상태로 폐기하는 기능
폐기단계	-	암호키가 명시적으로 폐기된 단계로 별도 기능이 요구되지 않음.
전체단계	감사	안전하게 관리되고 있는지 기록하고 감사하는 기능
	사고추적	사고발생시 원인을 추적할 수 있는 기능

키 관리 권고사항을 참조하여 OTP의 암호키 관리시의 상태와 기능에 따라 암호키 관리 단계 및 기능을 [표 2]과 같이 4단계로 분류하고, 각 단계별로 암호키 관리 기능에 대한 보안 요구사항을 정의하고 있다.

2.1.3 OTP 검증서버를 위한 응용 프로그램 인터페이스 (TTAK.KO-12.0132)

본 표준은[4] "PKCS#11 Mechanisms for One-Time Password Tokens"와 RSA Security의 "A CryptoAPI Profile for One-Time Password Tokens"를 참조하여 OTP 검증 서버를 구현하기 위해 필요한 공통적인 기능을 분석하고, 상호 연동성을 보장하는 응용 프로그램 인터페이스를 정의한 표준이며, API를 [표 3]에 표기한 것과 같이 핵심 모듈 API, 인증모듈 API, 검증 서버 API로 분류하여 설명하고 있다.

〔표 3〕 OTP 검증서버를 위한 API

분류	설명
핵심 모듈 API	OTP 구동 알고리즘만을 포함하여 최소화된 핵심 모듈에서 제공하는 기능으로 OTP 생성, 인증/보정, 질의 값 생성의 총 3가지 기능
인증 모듈 API	핵심 모듈에 사용자 데이터베이스가 추가된 인증 모듈에서 제공하는 기능으로, 인증/보정, 동기화, 질의 값 생성의 총 3가지 기능
검증 서버 API	핵심 모듈을 포함하여 독립된 OTP 검증 서버에서 제공하는 기능으로 인증, 동기화, 보정, 질의 값 생성의 총 4가지 기능

2.2 국외 OTP 표준화 동향

국외 OTP 표준은 IETF, ITU-T SG17/Q.7에서 주로 진행하고 있다.

IETF에서는 1995년에 일회용패스워드 인증 워킹그룹이 설립되어 S/Key 기술을 일회용 패스워드 시스템 표준(RFC2289)으로 제정한 이래로, OTP 인증기술에 관련한 표준화 활동은 VeriSign사, IBM사, VASCO사 등 60여개의 업체가 참여하고 있는 인증기술 컨소시엄인 OATH(Open AuTHentication)와 RSA사를 중심으로 이루어지고 있다.

2005년에 OATH에서 제안한 HMAC 기반의 일회용 패스워드 알고리즘 표준(RFC4226)이 제정되었고, 2007년에는 RSA사가 제안한 EAP와 일회용패스워드 프로토콜을 결합한 표준(RFC4793)이 제정되었으며, OATH(Open AuTHentication)에서 제안한 시도-응답 방식의 일회용패스워드 알고리즘과 시간 동기화방식의 일회용패스워드 알고리즘에 관한 스펙, RSA사에서 제안한 Kerberos에 일회용패스워드를 적용한 프로토콜과 TLS에 일회용패스워드를 적용한 프로토콜 등이 현재 IETF 인터넷드래프트 버전으로 있다.

ITU-T에서는 SG17/Q.7에서 2011년 2월 '일회용 패스워드 기반 인증 프레임워크 표준(X.1153)'이 제정되었고, 현재는 '일회용 패스워드 기반의 부인방지 프레임워크' 표준화가 진행 중에 있다. 다음 [표 4]는 국외에서 제정된 OTP 관련 표준을 나타낸다.

〔표 4〕 국외 OTP 표준

표준 제목	표준번호
A One-Time Password System	IETF RFC2289
HOTP: An HMAC-Based One-Time Password Algorithm	IETF RFC4226
PKCS #11 Mechanisms for One-Time Password Tokens	PKCS #11 v.2.20
Cryptographic Token Key Initialization Protocol	IETF RFC4758
XKMS Provisioning of OATH Shared Secret Keys	IETF Internet Draft
OTP Methods for TLS	IETF Internet Draft
The EAP Protected One-Time Password Protocol	IETF RFC4793
OCRA: OATH Challenge-Response Algorithms	IETF Internet Draft
TOTP: Time-based One-time Password Algorithm	IETF RFC6238
Dynamic Symmetric Key Provisioning Protocol	IETF RFC6063
Portable Symmetric Key Container	IETF RFC6030
The management framework of OTP-based authentication services	ITU-T X.1153
An One time password based non-repudiation framework	ITU-T X.sap-6(진행중)

2.2.1 OTP Methods for TLS (IETF Internet Draft)

본 표준안은[5] 현재 IETF의 인터넷 드래프트 버전으로 인터넷 전송 계층의 보안 프로토콜인 TLS(Transport Layer Security)에서 OTP를 이용한 PSK(Pre-Shared Key)를 생성하는 2가지 방식을 정의한다. 첫 번째 방식

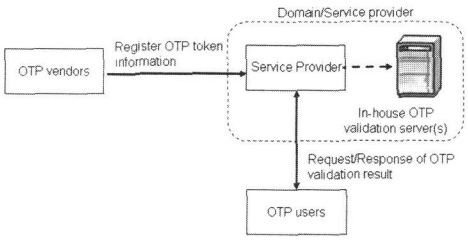
은 OTP를 바로 PSK로 사용하는 방법이고, 다른 한가지는 OTP를 이용해서 PSK를 유도하는 방식이다. Direct use with entropy-enhancing PSK ciphersuites 방식은 OTP를 PSK로 바로 사용하는 방식으로 TLS에 정의된 키 교환 알고리즘 중 DHE-PSK 또는 RSA_PSK와 같이 적용될 수 있지만, DHE-PSK의 경우 MITM(Man-In-The-Middle) 공격에 취약할 수 있기 때문에, 별도의 서버 인증 등의 방법이 없는 경우는 권고하지 않고 있다. Deriving a PSK through OTP hardening 방식은 OTP를 이용해서 PSK를 유도하는 방식으로 키 유도 메커니즘은 PKCS #5 V2.0의 PBKDF2를 권고하고 있다. 이 방식은 TLS에 정의된 모든 키 교환 알고리즘과 같이 사용 될 수 있다.

본 표준에서는 PSK 생성 방식을 추가하면서, 기존 TLS에 다음의 2개의 확장(extension) 타입을 정의한다. OTP challenge data extension은 챌린지(challenge)를 이용해서 OTP를 생성시 필요한 확장 타입으로, OTP 생성 전에 챌린지 값을 얻어와야 하기 때문에 Client Hello 메시지와 Server Hello 메시지의 확장 필드에 OTP challenge data extension을 추가한다. OTP hardening extension은 OTP를 이용해서 PSK를 유도하고자 할 경우 해당 확장 필드를 사용하며, 키 유도를 위한 iteration count 정보를 포함하고 있다. 해당 확장 필드는 Client Hello 메시지와 Server Hello 메시지의 확장 필드에 포함하며, 이렇게 공유한 정보를 이용해서 PSK를 유도하는 방법을 정의한다.

2.2.2 The management framework of OTP-based authentication services (ITU-T X.1153)

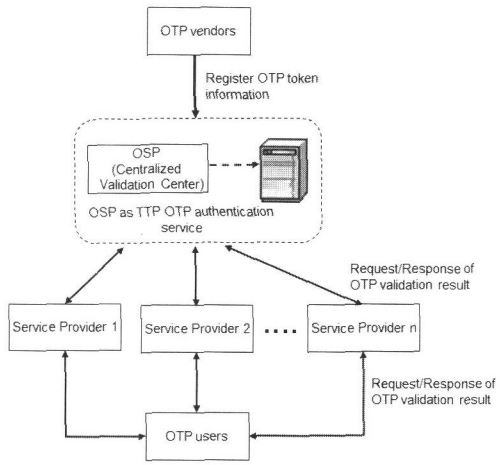
본 표준은[6] 2011년 2월 ITU-T X.1153으로 등록된 OTP 기반의 인증 서비스를 위한 관리 프레임워크로 basic, Centralized, Enhanced centralized, Cross-domain의 4가지 관리 모델에 따라 각각의 프레임워크를 정의 하고 있다.

Basic 관리 모델은 [그림 2]와 같으며 가장 기본이 되는 모델로 본 모델의 장점은 서비스제공자의 상황에 가장 이상적인 시스템 구성이 가능하다는 것이다. 그러나 사용자는 서비스제공자가 발급한 OTP 기기를 다른 서비스에서 사용할 수 없어서 2개 이상의 서비스제공자에게 가입한 사용자는 다수의 OTP 기기를 소지해야 하는 불편함이 있다.



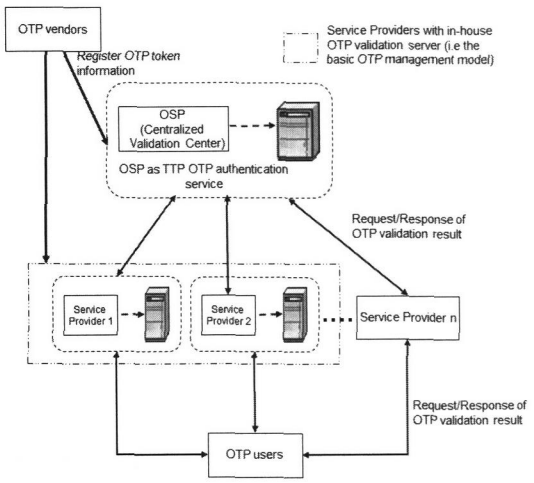
〔그림 2〕 Basic 관리 모델

Centralized 관리 모델은 [그림 3]와 같이 사용자는 하나의 OTP 기기를 여러 서비스제공자들에게 이용 등록하여 여러 서비스제공자들의 서비스를 이용하는데 사용할 수 있다. TTP는 모든 인증 요청을 중앙집중적으로 관리하므로 신뢰된 자에 의해 운영되어야 한다. 이 모델의 장점은 서비스제공자가 인증서버를 구축하지 않아도 OTP 인증을 제공할 수 있다는 것으로 서비스제공자는 구축비용을 절감할 수 있으며, TTP가 지원하는 다양한 종류의 OTP 기기를 모두 사용할 수 있다. 사용자의 입장에서는 다수의 서비스제공자에 가입되어 있는 경우, 1개의 OTP 기기로 여러 서비스제공자의 서비스들을 공통적으로 사용할 수 있어 편의성 측면이 우수하다. 반면에 단점으로는 모든 서비스 제공자의 인증요청 및 상태확인을 TTP에 중앙 집중적으로 요청하여야 한다는 점으로, TTP 장애가 발생하는 경우 연결된 모든 서비스 제공자에 영향을 주어 서비스 장애가 발생할 수 있다.



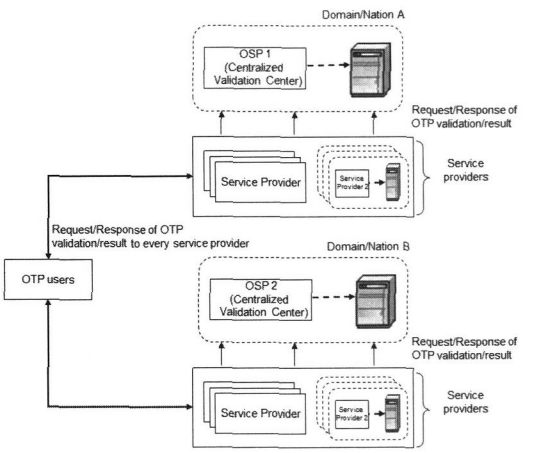
〔그림 3〕 Centralized 관리 모델

[그림 4]의 Enhanced centralized 관리 모델은 위의 centralized 관리 모델의 단점을 보완한 모델로 TTP에 중앙집중적으로 요청되는 것을 서비스제공자 내부에서 선택적으로 구축한 대체인증서버를 이용해서 분산하는 방식이다.



〔그림 4〕 Enhanced centralized 관리 모델

[그림 5]은 cross-domain 관리 모델로 서로 다른 도메인에 존재하는 TTP간의 연동으로 기존 시스템의 변동 없이 가능한 모델이다.



〔그림 5〕 cross-domain 관리 모델

2.2.3 An One time password based non-repudiation framework (ITU-T X.sap-6)

본 표준안은[7] 현재 ITU-T SG17/Q.7에서 표준화 중이다. OTP를 이용한 전자거래 시 OTP 사용자, 서비스 제공자간에 데이터 송신 또는 수신에 대한 부인을 방지하기 위해 신뢰된 제3자(TTP)를 통해 기능을 제공하고 이를 위한 OTP 기반의 부인방지 프레임워크를 정의하고 있다.

본 표준은 OTP기반 부인방지 서비스 시에 필요한 적용 시나리오와 프레임워크에 필요한 각 객체들을 정의하고 부인방지 토큰과 부인방지 처리 절차를 정의한다. 또한 OTP기반 부인방지 서비스 시에 필요한 보안 요구사항을 정의하고, 부인방지 토큰을 생성한 방법을 정의하고 있다.

Ⅲ. 동향 분석

3.1 OTP 표준화의 분류

본 절에서는 OTP의 표준화 동향을 분석하기 위해서 아래의 [그림 6]과 같이 OTP 관련 표준의 특성에 따라 4가지 항목으로 분류한다.

〔그림 6〕 OTP 표준의 분류

"OTP 보안관리"는 OTP의 보안성을 확보하기 위한 가이드라인 관련 표준들을 분류한다. 'OTP 암호키 관리 보안 요구사항', 'OTP 발생기 보안 요구사항'등이 여기에 속한다. "OTP 서비스 프레임워크"는 통합인증서비스를 위한 기본적인 프레임워크 관련 표준을 분류한다. 해당 표준으로는 ITU-T X.1153 'OTP기반 인증서비스 관리 프레임워크' 등이 있다. "OTP 시스템"은 OTP 기반 인증서비스의 상호 연동성을 보장하기 위한 시스템 기술 규격을 분류한다. 'OTP 암호키 컨테이너',

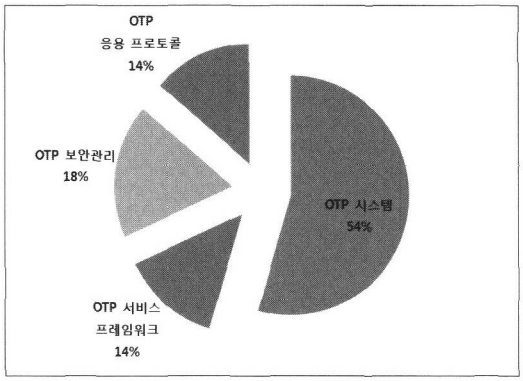
〔표 5〕 국내·외 OTP 관련 표준의 분류

분류	표준 제목	표준번호
OTP 보안관리	일회용 패스워드(OTP) 암호키 관리 보안 요구사항	TTAK.KO-12.0100
	일회용 패스워드(OTP) 토큰 보안 요구사항	TTAK.KO-12.0130
	일회용 패스워드(OTP) 인증서비스를 위한 보증 레벨	TTAK.KO-12.0120
	일회용 패스워드(OTP) 검증 서버 보안요구사항	TTAK.KO-12.0169
OTP 서비스 프레임워크	OTP 통합인증 서비스 프레임워크	TTAK.KO-12.0128
	The management framework of OTP-based authentication services	ITU-T X.1153
	An One time passwod based Non-repudiaion framework	ITU-T X.sap-6
OTP 시스템	A One-Time Password System	IETF RFC2289
	HOTP : An HMAC-Based One-Time Password Algorithm	IETF RFC4226
	PKCS#11 Mechanisms for One-Time Password Tokens	PKCS#11 v2.20
	Cryptographic Token Key Initialization Protocol	IETF RFC4758
	XKMS Provisioning of OATH Shared Secret Keys	IETF Internet Draft
	OCRA: OATH Challenge-Response Algorithms	IETF Internet Draft
	TOTP : Time-based One-time Password Algorithm	IETF RFC6238
	Dynamic Symmetric Key Provisioning Protocol	IETF RFC6063
	Portable Symmetric Key Container	IETF RFC6030
	일회용 패스워드(OTP) 키 컨테이너	TTAK.KO-12.0129
	일회용 패스워드(OTP) 검증서버를 위한 응용 프로그램 인터페이스	TTAK.KO-12.0132
	일회용 패스워드(OTP) 기반 인증 서비스 관리 프로토콜	TTAK.KO-12.0168
OTP 응용프로토콜	OTP Methods for TLS	IETF Internet Draft
	The EAP Protected One-Time Password Protocol	IETF RFC4793
	일회용 패스워드(OTP) 기반 전자금융 거래검증 프로토콜	TTAK.KO-12.0167

'OTP 검증서버를 위한 응용 프로그램 인터페이스' 표준이 여기에 해당한다. 마지막으로 "OTP 응용 프로토콜"은 OTP 기반의 확장 응용프로토콜을 관련 표준을 분류한다. 'OTP 기반 전자금융 거래검증 프로토콜'등이 여기에 해당한다.

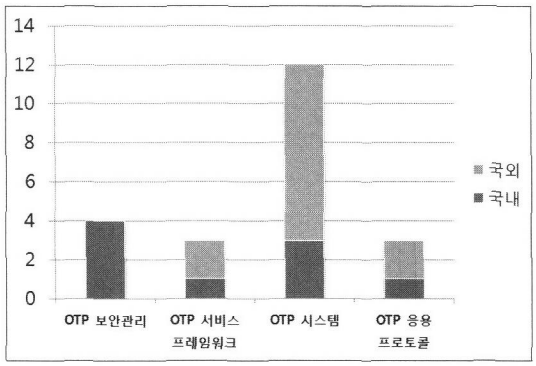
3.2 OTP 표준화의 분석

국내·외 OTP 관련 표준의 분석 결과 [그림 7]와 같이 OTP의 상호 연동성을 보장하기 위한 "OTP 시스템" 관련 표준이 가장 많이 제정되었으며, 그 다음으로 OTP의 보안성 확보를 위한 "OTP 보안관리" 표준이 제정되었다. 통합서비스를 위한 "OTP 서비스 프레임워크 표준"와 OTP 응용서비스를 위한 "OTP 응용 프로토콜"은 가장 낮게 제정되었다.



〔그림 7〕 OTP 표준 분석

국내 전자금융 환경에 OTP 기반의 인증 서비스가 활성화 되어 있는 특성 때문에 [그림 8]에서 볼 수 있듯이 실 서비스에 필요한 OTP 보안관리 표준은 국내 표준만



〔그림 8〕 OTP 국내·외 표준 분석

4건 제정된 상태이며, 통합서비스를 위한 OTP 서비스 프레임워크 표준은 국내 금융보안연구원에서 국내 · 외 표준 3건을 모두 주도적으로 추진하고 있다.

국내에서는 실 서비스에 필요한 OTP 보안 관리와 OTP 서비스 프레임워크 표준이 주도적으로 추진되고 있는 반면, OTP 응용프로토콜 관련 표준화는 아직까지 미흡한 것으로 나타났다.

국내에서 OTP의 활용 범위가 산업계 전반에서 점점 더 넓혀 가고 있기 때문에 앞으로는 보급된 OTP 발생기를 활용할 수 있는 "OTP 응용 프로토콜"과 관련된 표준화 및 기술이 증가될 것으로 보인다.

Ⅳ. 결 론

본 논문에서는 국내 · 외에서 제정되었거나 진행되고 있는 OTP 표준을 조사하여 대표적인 표준을 분석하고 표준화 동향을 살펴보았다.

국내는 TTA 에서 금융보안연구원이 OTP 표준화를 주도하고 있었으며, 국외 OTP 표준은 IETF에서 VeriSign사, IBM사, VASCO사 등 60여개의 업체가 참여하고 있는 인증기술 컨소시엄인 OATH(Open Au THentication)와 RSA사를 중심으로 이루어지고 있다. 또한, ITU-T에서는 SG17/Q.7에서 금융보안연구원 주도로 2011년 2월 '일회용 패스워드 기반 인증 프레임워크 표준(X.1153)'이 제정되었고, 현재는 '일회용 패스워드 기반의 부인방지 프레임워크'(X.sap-6) 표준화가 진행 중에 있다.

이와 같이 앞으로도 국내 · 외에서 스마트 환경에 적합한 OTP 기술 등의 활발한 표준화 작업이 진행 될 것으로 보이며, 이를 밑바탕으로 산업계에서도 기술 활성화가 진행될 것으로 기대된다.

참고문헌

[1] 금융보안연구원, "OTP 발급량 집계", *내부자료*, Mar 2012.

[2] 한국정보통신기술협회, "일회용패스워드(OTP) 통합인증 서비스 프레임워크", *TTAK.KO-12.0128*, Dec 2009.

[3] 한국정보통신기술협회, "일회용패스워드(OTP) 암호키 관리 보안 요구사항", *TTAK.KO-12.0100*, Dec 2009.

[4] 한국정보통신기술협회, "일회용패스워드(OTP) 검증서버를 위한 응용 프로그램 인터페이스", *TTAK.KO-12.0132*, Dec 2010.

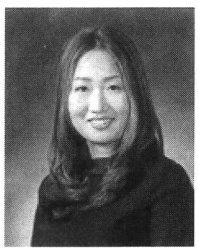
[5] J. Linn, M. Nystroem, "OTP Methods for TLS", *IETF Netwok Working Group,* June 2006.

[6] ITU-T, "A management framework of an one time password-based authentication service" *X.1153,* Feb 2011.

[7] ITU-T, "An One time password based non-repudiation framework" *X.sap-6* Feb 2012.

〈著者紹介〉

송 성 현 (Song Seong Hyeon)
2009년 7월: 세종대학교 컴퓨터공학과 석사
2011년 8월~현재: 전남대학교 컴퓨터공학과 박사
2010년 3월~현재: 금융보안연구원 인증기술팀 주임연구원
<관심분야> 프로토콜, 인증, 네트워크 보안



김 근 옥 (Kim Keun Ok)
준회원
2004년 2월: 성균관대학교 전자전기 컴퓨터공학과 석사
2011년 8월~현재: 성균관대학교 전자전기 컴퓨터공학과 박사과정
2010년 3월~현재: 금융보안연구원 인증기술팀 주임연구원
<관심분야> 전자공학, 통신공학, 정보보호