情 報 保 護 學 會 誌
第17卷 第3號, 2007. 6

OTP 기술현황 및 국내 금융권 OTP 도입사례

서승현*, 강우진**

요 약

지난해 말 전자금융 서비스 가입자 수가 6500만 명을 넘어섰으며, 올해로 도입 10년째를 맞이하고 있는 인터넷 뱅킹 서비스는 유비쿼터스 시대와 맞물려 우리 생활 깊숙이 자리 잡았다. 은행을 방문하지 않아도 일상생활에서 쉽게 접할 수 있는 전자매체를 통해 금융거래를 할 수 있다는 편리함으로 전자금융서비스를 이용한 거래가 창구거래보다 높은 상황이며, 전자금융거래 이용도는 계속 증가할 전망이다. 그러나 이러한 편리함 이면에는, 전자금융의 보안 허점을 노린 해킹시도가 끊이지 않고 있으며, 2005년 5월 인터넷 뱅킹 사고를 시작으로, 2007년 1월 대형 은행 고객정보 대량 유출 피싱 사건, 2007년 2월 공인인증서 유출로 인한 은행 불법 인출 사건 등 금전적인 이득을 노린 금융보안 사고들이 발생하고 있다. 최근 정부에서는 이러한 보안위협으로부터 사용자의 금융정보를 보호하고, 안전한 전자금융서비스를 제공하고자 "전자금융거래 안전성강화 종합대책"을 발표하였고, 이의 일환으로 기존 보안카드보다 보안성이 높은 OTP 기기를 개인고객에게도 도입하도록 하는 방안을 추진하고 있다. 본 논문에서는 일반 전자금융 서비스 고객에게도 확대되어 사용될 것으로 기대되는 OTP 기기의 기술 현황 및 국내 금융권 OTP 도입사례를 살펴보도록 한다.

Ⅰ. 서 론

2005년 5월 국내 최초로 발생한 인터넷뱅킹 해킹 사고를 계기로, 산업자원부, 정보통신부, 금융감독위, 금융감독원은 공동으로 "전자금융거래 안전성강화 종합대책"[1]을 수립하여 2005년 9월 경제정책조정회의에 보고하였다.

"전자금융거래 안전성강화 종합대책"은 개인 정보유출로 인한 전자금융사고의 피해를 최소화하고, 안전한 전자금융거래를 위한 대책을 해킹방지 프로그램 분야, 전자거래시스템 운영 관리 분야, 공인인증서 관리체계 개선 분야로 나누어 제시하고 있다.

특히, 전자거래시스템 운영 관리 분야의 경우, 현재 35개의 비밀번호가 반복되어 사용되고 있는 보안카드의 취약성을 개선하기 위해, 1차적으로 보안카드 내에 2개의 비밀번호를 조합하는 방식을 이용하여 기존의 35개에서 870~1190개로 비밀번호를 확대해 사용하도록 하였고, 궁극적으로는 기존 보안카드 방식보다 보안성을 더욱 향상 시킨 OTP(One Time Password) 기기를 금융권에서 도입하도록 하였다. 이와 함께, OTP 통합인증센터를 설립하여, 금융권에서 사용할 공동의 OTP 인증 시스템을 개발하고 통합 운영 및 관리를 전담하도록 하였다.

이에, 국내 금융기관들은 OTP에 상당한 관심을 가지고, 2007년 6월말로 예정된 OTP 통합인증 서비스 오픈에 맞춰, OTP 기기 도입 및 OTP 인증을 위해 필요한 개발들을 활발히 진행하고 있는 중이다.

본 논문에서는 OTP 기술현황과 금융권 OTP 도입사례를 중점적으로 다루며, 세부 항목은 다음과 같다. 2장에서는 OTP 개요를 설명하고, 3장에서는 OTP 생성방식 종류를 소개하며, 4장에서는 OTP 기술을 도입하면서 고려해야할 보안 사항 등을 기술한다. 마지막으로 5장에서는 국내 금융권의 OTP 도입현황을 살펴보고, OTP 통합인증센터를 소개함으로써 결론을 맺는다.

Ⅱ. OTP 기술 개요

이 장에서는 사용할 때마다 매번 다른 비밀번호를 생성해내는 OTP 기기의 특성 및 기존 비밀번호 인증방식과의 차이점 등을 기술하고, OTP에서 제공하는 2-factor 인증

* 금융보안연구원 인증관리팀 (seosh@fsa.or.kr)
** 금융보안연구원 인증관리팀 (hanull@fsa.or.kr)

방식, OTP 생성 단계, 생성 매체 종류 등을 알아본다.

2.1 OTP 개념 및 특성

OTP는 매번 다른 비밀번호로 사용자를 인증하는 일회용 비밀번호를 의미하며, 현재 사용하는 비밀번호로부터 다음번에 사용할 비밀번호를 유추하는 것이 수학적으로 불가능한 특성을 가진다[14].

기존의 패스워드를 사용한 인증 방식은 간편하고 편리하여 오랫동안 여러 응용시스템에서 사용자 인증 방식으로 사용되어져 왔다. 그러나 사용자들이 한번 만들고 나서 변경하지 않으면 영구적으로 사용가능한 정적인 패스워드(static password)는 보안성이 낮으며 쉽게 노출 가능한 불완전한 인증 방식이다. 보통 사용자들은 기억하기 쉽고 추측이 가능한 단어나 숫자들로 패스워드를 구성하기 때문에, 타인에 의해서 쉽게 유추가능하다. 그밖에도 공격자가 키로거, 네트워크 스니핑, 사전공격, 전수조사공격 등을 통해서 정적인 패스워드를 취득하고 나면 재사용이 가능하다는 취약점을 가지고 있다.

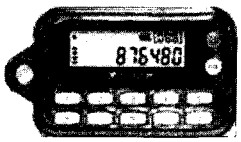
이와 달리, OTP는 의미 있는 단어, 숫자 패턴, 특정 사용자와 연관된 문자 등으로 구성되어있지 않아, 기억 가능하거나 쉽게 유추할 수 없다. 또한 매번 다른 비밀번호를 생성하는 동적인(dynamic) 특성을 갖기 때문에, 취득한 값을 재사용할 가능성이 희박하다. 그밖에도 PIN (Personal Identification Number)을 함께 사용하여 2-factor 인증을 제공할 수 있기 때문에 1-factor 인증방식인 정적인 패스워드 방식에 비해 더 안전하다고 할 수 있다.

2.1.1 OTP에서 제공하는 2-factor 인증

2-factor 인증 방식이란 사용자를 인증하는 세 가지 방법 (i)알고 있는 것 확인하는 방법(패스워드, PIN번호 등), (ii)소유하고 있는 것을 확인하는 방법(스마트카드, 보안카드, OTP기기 등), (iii)사용자 자신을 확인하는 방법(생체정보) 중에서 두 가지 방법을 조합해서 사용하는 인증 방식을 말한다. OTP기기는 PIN과 함께 사용하면 2-factor 인증((i)PIN번호 기억+(ii)OTP기기 소유)을 제공할 수 있으며, OTP에서 제공하는 PIN으로는 H/W PIN과 S/W PIN이 있다.

(1) H/W PIN

H/W PIN이 제공되는 OTP 기기란 OTP 기기에 PIN

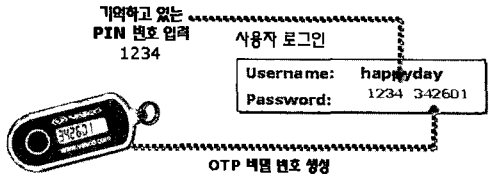


〔그림 1〕 H/W PIN을 제공하는 OTP 기기

번호를 입력할 수 있는 PIN 패드가 부착되어있어서, 사용자가 자신이 기억하고 있는 올바른 PIN번호를 OTP 기기에 입력해야만, 기기에서 생성된 OTP 값이 보여지는 형태의 기기를 의미한다. 사용자가 잘못된 PIN번호를 입력하면 OTP 값을 알 수 없으며, PIN 입력 오류횟수를 초과하게 될 경우, OTP 기기 자체가 잠김 상태로 바뀐다. 따라서 H/W PIN은 OTP 기기 분실 시 하드웨어 잠김 기능으로도 활용된다.

(2) S/W PIN

S/W PIN을 지원하는 OTP 기기는 기기에 별도의 PIN 패드가 부착되어 있지 않은 형태로, OTP 생성 값이 자동으로 보여지기 때문에, 기기의 잠금 기능이 제공되지 않는다. 대신 사용자는 사용자 인증 요청 시, 사용자가 알고 있는 S/W PIN번호와 함께 OTP 기기에서 생성된 OTP값을 입력해야 하고, 이 두가지 비밀 값이 모두 올바른 경우에만 사용자 인증이 성공하게 된다. 따라서 PIN번호를 모르는 상태에서 단순히 OTP기기 습득만으로는 OTP인증 승인을 받기 어렵다.



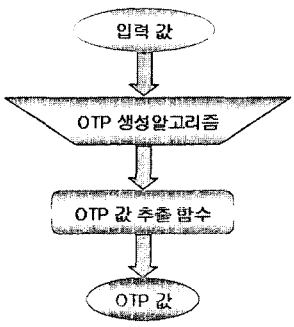
〔그림 2〕 S/W PIN을 제공하는 OTP 기기

2.2 OTP 생성 단계

OTP 값은 다음과 같은 생성단계를 거쳐 생성된다[12].

(1) 입력 값 : OTP 생성알고리즘의 입력 데이터

- 질의 · 응답 방식 : 질의값, 서버와 OTP기기 간에 공유된 비밀키 등
- 시간 동기화 방식 : 시간값, 서버와 OTP기기 간에 공유된 비밀키 등



〔그림 3〕 OTP 생성 단계

- 이벤트 동기화 방식 : 카운터(이벤트의 횟수), 서버와 OTP 기기 간에 공유된 비밀키 등
- 조합 방식 : 시간값, 카운터(이벤트의 횟수), 서버와 OTP 기기 간에 공유된 비밀키 등

(2) OTP 생성알고리즘: 입력 값으로부터 OTP 값을 생성해내는 알고리즘으로, 일방향 해쉬함수(출력으로부터 입력을 유추할 수 없는 함수)와 대칭키 암호화알고리즘(현재 블록암호알고리즘이 사용됨)에 기반 함

(3) OTP 값 추출 알고리즘(Truncate 함수): OTP 생성알고리즘을 통해 출력된 값으로부터 실제 OTP로 사용할 OTP 값 6~8자리 숫자를 뽑아내는 알고리즘

2.3 OTP 생성 매체의 종류

OTP를 생성하는 매체는 OTP 전용기기, 모바일 OTP, 카드형 OTP, 보이스 OTP 등이 있다.

(1) OTP 전용기기[3,4,6,7,8,10]

OTP를 생성할 수 있는 연산 기능, 암호 알고리즘, 입력값 등을 내장하고 있는 OTP 생성 전용의 하드웨어 매체로, 그 형태는 계산기, 열쇠고리, 목걸이, 호출기, USB 등으로 다양하다. OTP 전용기기는 추가 장비 필요없이 사용가능하여 시스템 적용이 용이하지만 사용자가 별도의 기기를 구매하여 휴대하고 다녀야하는 불편함이 있다.

(2) 모바일 OTP[3,4,5,6]

모바일 OTP는 OTP 생성알고리즘이 소프트웨어 모듈로 휴대폰에 탑재된 형태로서, 별도의 OTP 기기를 구매하여 휴대할 필요가 없는 장점을 가진다. 그러나 모바일 뱅킹 서비스에서는 이용이 불가능 하고, 휴대폰 복제를 통한 OTP 비밀키 유출가능성 S/W의 역공학(reverse engineering)을 통한 해킹, 키관리 부분에 있어서 취약성이 있다.

(3) 카드형 OTP[9,11]

IC 카드형 OTP 기기로, IC 카드 내에는 OTP 생성 모듈이 내장되어 있으며 디스플레이 창과 OTP 생성 버튼이 부착되어 있는 형태이다. IC 카드를 활용할 수 있으나 구입비용이 높다.

(4) 보이스 OTP[4,11]

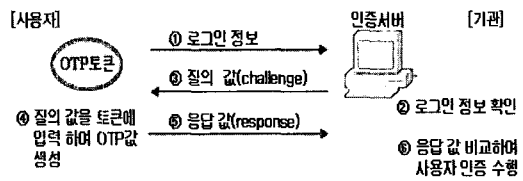
IC 카드에 OTP 생성 모듈, 배터리, 버튼, 스피커를 내장시켜 사용자가 버튼을 누르면 특정 소리가 생성되고 그 생성된 소리가 OTP로 사용된다. 노인, 시각장애인에게 효과적으로 적용할 수 있는 방식이나 마이크 장비 및 부가 장치들이 필요하고 구입비용이 높다.

Ⅲ. OTP 생성 방식의 종류

OTP 생성 방식은 OTP 기기와 인증 서버간의 동기화 여부에 따라 비동기화 방식과 동기화 방식으로 나뉜다.[2]

3.1 비동기화 방식

비동기화 방식의 OTP는 OTP 기기와 인증 서버간에 미리 설정되어 있는 동기화 기준 정보가 없어, 인증 요청시 사용자가 직접 임의의 난수 값을 OTP 기기에 입력하여 OTP 값을 생성하는 방식을 말한다. 비동기화 방식의 대표적인 예가 질의-응답(Challenge- Response)[13] 방식이며, 금융권에서 OTP 도입 초기에 주로 사용되었다.



〔그림 4〕 질의-응답 방식

질의-응답 방식은 사용자가 OTP 인증 요청시 인증서버로부터 받은 질의 값을 직접 OTP 기기에 입력하여 응답 값(난수 형태)을 생성하는 방식으로, 사용자가 로그인화면에 생성된 응답 값을 입력한다. 질의-응답 방식은 OTP 기기와 인증 서버 간에 동기화해야할 기준 정보가 없기 때문에, 동기화할 필요가 없으며, 사용자와 서버 간에 상호인증을 제공하는 방식으로 쉽게 확장이 가능하다는 장점을 가진다. 그러나, 사용자가 직접 질의 값을 OTP 기기에 입력하고, 생성된 응답 값을 로그인 화면에 입력해야한다는 불편이 있으며, 인증서버도 해당 사용자의 질의 값을 관리해야 하는 부담이 있다. 또한 일반적인 패스워드 인증 어플리케이션과 호환이 쉽지 않다.

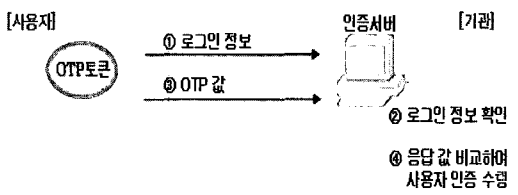
3.2 동기화 방식

동기화 방식의 OTP는 OTP 기기와 인증 서버 간에 미리 공유된 비밀정보와 동기화 정보에 의해 OTP 값이 생성되는 방식이다. 비동기화 방식에 비해, OTP 기기와 인증 서버간에 반드시 동기화가 이루워져야 올바른 인증 처리가 된다는 제약점이 있으나, 사용자 입력 불편, 기존 ID/PWD 어플리케이션과의 호환 어려움 등 비동기화 방식의 단점을 개선하였다.

OTP 입력 값의 하나인 동기화 정보에 따라 시간 동기화(time-synchronous), 이벤트 동기화(event-synchronous), 조합 방식으로 나눌 수 있으며, OTP 입력 값으로 시간 동기화 방식은 현재시간, 공유된 비밀키 값을 받고, 이벤트 동기화 방식의 경우, 이벤트 카운터 값과 공유된 비밀키 값을, 조합방식의 경우, 시간값, 이벤트 카운트 값, 공유된 비밀키 값을 받는다.

3.2.1 시간 동기화 방식

시간 동기화 방식은 서버와 OTP 기기 간에 동기화된 시간 정보를 기준으로 특정 시간간격(보통 1분)마다 변하는 비밀번호를 생성하는 방식이다.



〔그림 5〕 동기화 방식

이 방식은 사용자의 인증요청과 상관없이 1분 간격마다 OTP 값이 매번 바뀌므로, 1분 동안 입력하지 못할 경우, 중간에 패스워드가 바뀌어 다시 입력해야 하고, 실수로 OTP값을 잘못 입력하면 인증 재시도를 위해 특정 시간동안 기다려야하는 불편이 있다. 그러나 이러한 특성은 MITM (Main-In-The-Middle)[15] 공격으로 공격자가 의미있는 OTP 값을 얻어냈다 하더라도 1분이내에 사용해야 공격에 성공할 수 있다는 제약점이 되고, 타인의 OTP 값을 기록하였다가 이후에 재사용하여 성공할 가능성이 희박하다는 점 등 보안성을 향상시킬 수 있는 장점이 된다.

3.2.2 이벤트 동기화 방식

이벤트 동기화 방식은 서버와 OTP 기기가 동일한 카운트 값을 기준으로 비밀번호를 생성하는 방식이다. 동기화 기준값으로 사용되는 카운트 값은 현재 시간 정보와 달리, OTP 기기와 인증 서버만 알 수 있는 값이기 때문에, OTP 입력 값으로 비밀키 이외에 또 하나의 비밀정보가 입력되는 형태라 볼 수 있다.

이 방식은 OTP 값을 얻은 후, 다시 OTP 생성 요청을 할 때까지 비밀번호가 바뀌지 않기 때문에, 사용자가 입력하는데 편리한 측면은 있으나, 실수로 여러번 OTP 값을 생성시키고 나면, 서버와 OTP 기기 간에 카운트 값이 동기화되지 않아 이를 보정해야하는 문제가 있다. 또한, MITM 공격으로 공격자가 의미있는 OTP 값을 얻어냈을 경우, 혹은 타인의 OTP 값을 생성하여 기록하였을 경우, 정상적인 사용자가 다음번 인증요청을 수행하기 전까지 이를 재사용하여 공격을 성공할 수 있다. 다음번 인증요청이 즉시 이루어진다면 공격의 성공가능성이 희박하나, 그렇지 않은 경우, 성공할 가능성이 존재한다.

3.2.3 조합 방식

시간 동기화 방식과 이벤트 동기화 방식의 장점을 조합하여 구성한 방식으로, 시간 동기화 중심의 조합방식과 이벤트 동기화 중심의 조합방식으로 구분된다.

시간 동기화 중심의 조합 방식은 특정 시간간격(보통 24초~32초)마다 비밀번호가 다시 생성되며, 같은 시간간격 내에서 재시도시에는 카운트 값을 증가시켜서 비밀번호가 바뀌도록 하는 방식이다. 따라서 1분 동안은 생성된 OTP 값이 바뀌지 않는 시간 동기화 방식에 비

해 1분 이내에도 여러번 다른 비밀번호를 생성하여 활용할 수 있다.

이벤트 동기화 중심의 조합방식은 특정 시간에 발생한 카운터 값을 기준으로 비밀번호가 생성되며, 사용자가 이벤트 버튼을 눌러 생성 요청을 할 때마다 값이 바뀐다. 그러나 기존의 이벤트 동기화 방식과는 달리, 타인이 몰래 OTP 값을 임의로 생성하여 기록해 두고 이후에 재사용하는 공격을 시도한다 할지라도, 카운트 발생 시간과 서버에서 인증하기 위해 카운트를 발생시키는 시간이 차이가 있기 때문에 인증실패가 되며, 공격에 성공하기 힘들다. 이러한 조합방식은 기존의 시간 동기화 방식이나 이벤트 동기화 방식에 비해 보안성은 향상시킨 측면은 있으나, 인증서버와 OTP 기기 간에 동기화를 유지하는 것이 쉽지 않기 때문에, 편의성 측면은 다소 떨어지는 부분이 있다.

〔표 1〕 OTP 제품 현황

구분	회사명	제품명	생성방식	매체종류
국산	인터넷[3] 시큐리티	두리키	시간동기화	모바일 OTP
		Secure Token	시간동기화/질의-응답	OTP 전용기기
	미래[4] 테크놀로지	Time OTP	시간동기화	OTP 전용기기
		Any OTP	시간동기화	카드형/보이스 OTP
		U-OTP	시간동기화	모바일 OTP
	이니텍[5]	INISAFE Mobile OTP	조합방식(T)	모바일 OTP
외산	RSA[6]	SecurID	시간동기화	OTP 전용기기 /모바일 /카드형
	Secure[7] Computing	Safeword	이벤트동기화	OTP 전용기기
		Alpine	시간동기화	OTP 전용기기
	VASCO[8]	Digipass	시간동기화/조합방식(T)	OTP 전용기기
	InCard[9]	InCard	이벤트동기화	카드형 OTP
	Active[10] Identity	Mini	시간동기화/이벤트동기화	OTP 전용기기
	Identita[11]	Identita	조합방식(E)	카드형/보이스 OTP

※ 조합방식(T) : 시간동기화 중심의 조합방식,
조합방식(E) : 이벤트동기화 중심의 조합방식을 의미함

3.3. OTP 제품 현황

OTP 통합인증센터 설립과 고액 이체에 대한 OTP 사용 의무화로 금융권의 OTP 도입 바람이 확산된 가운데, 현재 국내 OTP 시장은 그 어느 때보다도 열기를 띄고 있으며, 대규모 시장형성이 예측되고 있다.

국내 기업 및 금융권에서 기 도입되어 사용되고 있거나, 도입을 검토 중인 OTP 제품 현황은 다음과 같다.

Ⅳ. OTP의 보안 고려사항

OTP 생성알고리즘의 기본적인 특성상, OTP 기기에서 생성되는 OTP 값은 랜덤성을 가지기 때문에 PIN번호 혹은 패스워드와 달리 의미있는 숫자나 단어로 구성되지 않아 쉽게 유추불가능하다.

기존의 전자금융거래에서 사용했던 보안카드는 35개 이내의 비밀번호가 반복적으로 사용되는 원리이기 때문에, 공인인증서가 누출되었을 경우, 네트워크 스니핑 혹은 키로거 등을 이용하여 해당 사용자의 보안카드 비밀번호를 일부 취득했을 때에도 공격이 성공할 수 있었다. 그러나 OTP는 매번 다른 비밀번호를 생성해내는 특성을 가지기 때문에, 사회 공학기법이나 네트워크 스니핑 등을 통해 의미있는 패스워드나 비밀번호를 얻어내어 재사용하였던 공격 방식을 무력하게 만든다.

또한, OTP 인증 시스템 자체에 대한 공격은 전수조사 공격을 통해 실제 사용되는 OTP 값을 얻어내는 것인데, 이는 시간적 제약이 있는 상황에서 000000 ~ 999999(6자리 OTP 값 기준)까지의 값을 대입할 수 있어야하므로 공격 성공확률이 $1/10^6$로 이론적으로 낮다고 할 수 있다. 8자리의 OTP 값을 사용하는 경우, 이 확률은 $1/10^8$로 더 떨어지게 된다[12,14]. 현재, 전자금융거래 시 3~5회 이상 연속 인증 실패를 하면 잠금 기능이 제공되기 때문에 무제한적인 인증시도는 불가능한 상황이라 할 수 있다.

따라서, 현재 소개되고 있는 OTP 인증 시스템의 해킹 방법들은 OTP 인증 시스템 자체를 깨는 것이 아니라, 피싱 공격이나 MITM 공격 등의 상황적 변수를 바탕으로 한 공격들로 볼 수 있다. 실제적으로 피싱이나 MITM 공격등에 대응하기 위해서는 사용자와 서버간의 상호 인증을 반드시 제공해야하며, 이는 OTP 인증 방식만으로는 해결이 어렵다.

즉, 피싱 공격에 대한 방어는 고객의 피싱에 대한 인

식제고, 공식 대화채널 사전검증(발신자의 신뢰성을 수신자가 확인할 수 있는 기능 제공), 보안을 고려한 웹 어플리케이션의 개발 및 웹 어플리케이션의 주기적 취약성 확인 등의 피싱 공격을 대비한 여러 방법들을 함께 이용해야 한다. 또한 MITM 공격에 대한 방어는 인증서버와 사용자간에 확실한 상호 인증 제공만이 해결책이며, 이를 지원할 수 있는 방법들을 이용해야 한다.

최근 금융기관들은 각종 금융보안 위협에 대응하기 위해서, PKI기반 솔루션, 키보드보안 프로그램에 이어 안티 피싱 및 파밍 솔루션 등 여러 보안 솔루션들을 도입하고 있는 상황이다. 이러한 방어책과 함께 OTP를 이용하게 된다면, 기존의 전자금융거래에서 문제가 되었던 보안 허점 및 취약점들이 상당히 개선될 것으로 보인다.

V. 금융기관 OTP 도입 현황

이 장에서는 국내 금융기관들의 OTP 이용 현황 및 도입 사례를 살펴보고, 현재 국내 금융권뿐만 아니라 해외 금융권에서도 큰 관심을 보이고 있는 OTP 통합인증센터에 대한 소개를 개략적으로 한다.

5.1 국내 금융기관 OTP 도입 현황

1990년대 말부터 국내의 몇몇 은행들이 기업 고객이나 일부 VIP 고객 대상으로 OTP를 도입하여 사용하고 있었으며, 초기에 도입했던 OTP 방식은 질의-응답 방식이었다. 최근 발표된 전자금융거래 안전성강화 종합대책에 따라 전자금융 거래시 OTP를 사용하면 고액 이체거래(1회 이체한도 5,000만 원 초과 1억 원 이하)를 할 수 있도록 함으로써[1], 금융권에서는 OTP 도입에 적극적인 모습을 보이고 있다.

이미 OTP를 도입하여 사용하고 있는 우리은행, 신한은행, SC제일은행, 기업은행, 외환은행, 농협, 씨티은행 등은 기업고객에 이어 개인 고객에까지 OTP 도입을 확대하고 있다. 2006년 12월 신한은행이 조흥은행과의 전산통합을 기념해 인터넷뱅킹 고객에게 OTP 단말기를 무료로 배포하면서 다수의 개인고객들이 OTP를 이용하고 있으며, HSBC 서울지점의 경우 개인고객의 OTP 사용을 의무화하여 시행하고 있다.

현재 OTP 통합인증센터 구축 및 서비스 개시 일정이 구체화되면서, 국민, 농협, 우리, 신한, 하나, 외환, SC제일, 씨티, 기업, 산업, 부산, 대구, 광주, 전북, 경남, 제주, HSBC, 수협 등 은행 19군데, 현대, 대우, 대신, 삼성, 교보, 미래에셋, 키움닷컴, 우리투자증권 등 증권사 30군데, 한맥선물, 신협, 저축은행 중앙회 등 기타권역 4군데를 포함하여 우체국, 새마을금고연합회까지, 총 55개 기관들이 OTP 통합인증센터 참여를 신청하였고 OTP 인증서비스 개발을 진행하고 있다.

〔표 2〕 국내 금융기관 OTP 도입 현황 (2007년 1월)

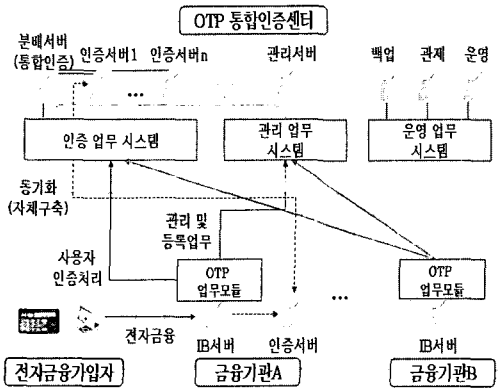
은행명	적용대상	매체종류
신한	개인/기업	OTP 전용기기
농협	개인/기업	OTP 전용기기, 모바일 OTP
우리	개인/기업	OTP 전용기기
기업	개인/기업	OTP 전용기기
씨티	기업	OTP 전용기기
SC제일	개인/기업	OTP 전용기기
외환	개인/기업	OTP 전용기기
광주	기업	OTP 전용기기
경남	기업	OTP 전용기기
전북	기업	OTP 전용기기
HSBC	개인/기업	OTP 전용기기

2007년 6월말, OTP 통합인증 서비스가 예정대로 개시되면, 1차적으로 은행 8군데, 증권사 6군데 정도가 개인고객 대상으로 OTP 인증서비스를 제공할 것으로 보이며, 2007년 9월이면 OTP 통합인증센터에 참여하는 55개 전금융기관이 OTP 인증서비스를 개인 및 기업 고객을 대상으로 제공하게 될 예정이다.

5.2 OTP 통합인증센터

인터넷뱅킹 해킹사고 및 각종 금전 이득을 노린 금융보안 사고들이 발생하면서, 전자 금융거래시 사용하였던 공인인증서 비밀번호, 계좌이체 비밀번호, 보안카드 비밀번호의 안전성에 대한 검토가 제기되었다. 이에 정부에서는 전자금융거래 안전성 강화 대책을 마련하고서 고액 이체에 한에서는, 기존 보안카드의 취약성을 개선한 OTP를 도입하여 사용하도록 하였다.

생성방식이나 매체의 종류가 다양한 OTP 기기를 금융기관마다 개별로 구축하여, 해당 금융기관에서만 사용이 가능하다고 한다면, 금융기관 4~5곳을 이용하는 사용자의 경우, 각 기관마다 OTP 기기를 발급받아



〔그림 6〕 OTP 통합인증센터 논리적 구성도

4~5개나 되는 기기들을 소유하고 다녀야 하기 때문에 매우 불편하게 된다. 또한 기기 구입에 대한 비용 부담도 크다.

따라서 정부는 개별 금융기관이 OTP 인증 시스템을 자체 도입하여, 구축하고 운영하는 데에 따른 부담을 최소화하고, 금융기관 간 OTP 사용의 호환성을 높여 사용자 편의성을 증가시키기 위해 OTP 통합인증센터 설립을 추진하였다.

OTP 통합인증이란 사용자가 하나의 OTP 기기를 가지고서도 자신이 거래하고 있는 모든 금융기관의 전자금융서비스를 이용할 수 있도록, 금융기관 공동으로 OTP 인증을 제공하는 것을 의미한다. 즉 금융기관 공동으로 구축하는 OTP 통합인증센터를 통해 전자금융 사용자의 OTP 통합인증이 수행되게 된다. 2007년 6월말 OTP 통합인증이 최초로 개시될 예정이며 금융기관의 1,2차 서비스 참여 기간을 거쳐, 다가오는 8월이면 OTP 통합인증센터에 참여 신청을 한 55개 금융기관은 모두 OTP 인증 서비스를 제공하게 될 예정이다.

Ⅵ. 결 론

언제 어디서나 쉽게 접근할 수 있는 전자 매체를 이용한 전자금융거래는 그 편리함으로 인하여, 해마다 그 거래 건수가 늘고 있으며, 이제는 전자금융 거래 비중이 창구 거래 비중보다 높다는 사실이 더 이상 놀랄만한 일이 아니게 되었다.

그러나 전자금융거래가 활발해짐에 따라, 금전적인 이득을 노린 보안사고도 기승을 부리고 있어, 이용자들의 불안을 야기하고 있으며, 이에 대응하기 위한 금융권의 노력도 분주해지고 있다. OTP 기기도 이런 대응책 중에 하나이며, 본 논문에서는 OTP 기술동향과 금융권의 OTP 도입현황을 살펴보았다.

OTP 통합인증센터가 본격적으로 가동되어, 기존 보안카드에 비해서 비밀번호 도용의 위험가능성이 희박한 OTP를 일반인들에게까지 확대 보급하여 사용하게 된다면, 보다 안전한 전자금융거래를 기대해볼 수 있는 것이 사실이다.

그러나 금융시스템에 대한 해킹기법도 날로 교묘해지고 있으며 그 공격방식도 다양하기 때문에, OTP 기술만으로 모든 금융 보안위협들에 대응할 수 있는 것은 분명 아니다. 이와 더불어, 안전한 전자금융 거래를 제공하기 위해서는 고객의 보안인식 제고, 여러 보안 솔루션 제공과 보안정책 수립 및 이행 등이 이뤄져야 할 것이다.

참고문헌

〔1〕 금융감독원, "전자거래 안전성 강화 종합대책", 2005.9.
〔2〕 백미연, "전자금융거래의 보안 강화 방안 및 OTP (One Time Password) 이용현황, 지급결제와 정보기술, 2006.4.
〔3〕 www.security.co.kr, 인터넷시큐리티사
〔4〕 www.miraetechnology.com, 미래테크놀로지사
〔5〕 www.initech.com, 이니텍사
〔6〕 www.rsa.com, RSA사
〔7〕 www.securecomputing.com, SecureComputing사
〔8〕 www.vasco.com, VASCO사
〔9〕 www.incardtech.com, InCard사
〔10〕 www.activeidentity.com, ActiveIdentity사
〔11〕 www.identita.com, Identita사
〔12〕 MRaihi, D., "HOTP: An HMAC-Based One Time Password Algorithm:, IETF RFC 4226, 2005. 12.
〔13〕 MRaihi, D., "OCRA: OATH Challenge Response Algorithm", IETF Internet Draft Informational, 2005. 12.
〔14〕 N. Haller, "A One-Time Password Standard", IETF RFC 1938, 1996.
〔15〕 A. J. Menezes, P. C. Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC, 1997.

〈著者紹介〉

서 승 현 (Seung-Hyun Seo)
종신회원
2000년 2월: 이화여자대학교 수학과 졸업 (학사)
2002년 2월: 이화여자대학교 컴퓨터학과 졸업 (석사)
2006년 2월: 이화여자대학교 컴퓨터학과 졸업 (박사)
2006년 5월~2007년 11월: 고려대학교 정보경영공학전문대학원 연구전임강사
2006년 12월 ~ 현재: 금융보안연구원 인증관리팀 주임연구원
관심분야: 암호이론, 네트워크보안, OTP

강 우 진 (Woojin Kang)
정회원
1992년 2월: 연세대학교 중어중문학과 졸업
1992년 2월 ~ 1998년 7월: 조흥은행 전산부
1999년 4월 ~ 2003년 1월: 투나인 정보기술 연구소장
2003년 4월 ~ 2006년 10월: LG CNS 금융사업부 전자금융업무 BA
2006년 11월~현재 : 금융보안연구원 인증관리팀장
관심분야 : 소프트웨어공학, 보안감리, 정보보호