정 보 보 호 학 회 지
제27권 제6호, 2017. 12

금융권에서 인증 보증 등급을 기반으로 한 신뢰 승급 방법

김 지 혜*, 사 경 진*, 염 흥 열**

요 약

최근 금융권에서는 고객의 편리성을 높이기 위해서 여러 인증 수단으로 서비스를 제공하고 있다. 본 논문은 인증 수단을 네 가지의 보증 등급으로 통제 수단에 따라 나누어 제시한다. 보증 등급을 토대로 등급별 신뢰 승급이 가능한 보안 정책을 제안하고 주로 사용될 금융서비스의 인증 수단을 강도로 나눈다. 또한, 신뢰 승급의 활용사례를 기술하면서 안정적으로 금융서비스에서 신뢰 승급 기반으로 인증을 사용할 수 있다.

Ⅰ. 서 론

국내의 금융권은 여러 인증 수단을 사용하여 서비스를 제공하고 있다. 현재 해외 표준에는 금융서비스에 대하여 인증 보증 등급이 3단계로 제시되어있고 각 보증 등급에 따라 위험 등급에 분류하여 그에 맞는 인증 수단을 금융서비스에 제시하고 있다. 그러나 우리나라는 현재 인증 보증 등급에 추가적인 신뢰 승급이 가능한 보안 정책과 인증 수단이 마련되어있지 않은 실정이다. 이에 따라 본 논문은 해외 표준(NIST SP800-63)을 참고하여 3단계의 보증 등급을 한국의 금융권 실정에 맞게 4단계의 보증 등급으로 제시한다.

본 논문에서는 현재 사용 중인 인증 보증 등급에 위험 등급에 따른 신뢰 승급 절차를 알아보려고 한다. 논문의 구성은 2장에서는 신뢰 등급 개요로 인증수단이 분류와 신뢰 승급의 개요 그리고 신뢰 승급의 필요성에 대해 다루고, 3장에서는 신뢰 승급의 절차를, 4장에서는 신뢰 승급이 가능한 보안 정책을 다룬다. 5장에 금융 서비스에 활용 가능한 인증 수단별 엔트로피 산정 방법과 강도의 신뢰 승급에 대해 알아본다. 6장에서는 실제 금융 서비스에 적용하여 신뢰 승급이 가능한 사례를 도식화 하였고, 마지막으로 7장에서 결론을 맺는다.

Ⅱ 신뢰 등급 개요

2.1. 인증 수단의 분류

인증 수단은 4가지 팩터로 구분할 수 있다. 각 팩터는 지식, 소지, 바이오생체, 바이오행위로 구분된다. 각각의 인증 수단별 예시는 아래의 〔표 1〕와 같다.

〔표 1〕 팩터별 인증수단 예시

팩터		인증수단 예시
지식		아이디/비밀번호, PIN
소지		OTP, 공인인증서
바이오	생체	얼굴, 홍채, 지문, 정맥
	행위	음성, 키스트로크, 마우스 움직임

2.2. 신뢰 승급 개요

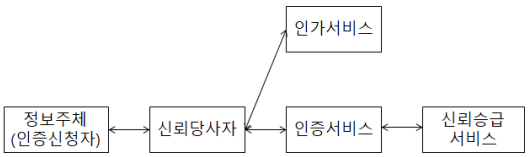
신뢰 승급은 이용하는 거래의 인증 등급이 현재의 인증된 등급보다 높은 인증 등급이 필요할 때, 추가적인 인증을 요구한다. 신뢰 승급은 인증 방법의 보증 등급별 관리 사항을 제시하여 서비스 상황별로 적합한 인증 방법을 선택할 수 있는 지침을 제공하는 것을 목적으로 한다.

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2015-0-00168, 상황인지기반 멀티팩터 인증 및 전자서명을 제공하는 범용인증플랫폼기술 개발)
* 순천향대학교 융합서비스보안학과 (ngswma32@gmail.com, kjin5831@gmail.com)
** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

이를 통해 여러 보안 위협에 대응하여 보안 등급별로 안전하게 인증 수단을 적용할 수 있을 것이다.

신뢰 승급을 하기 위해서는 다음의 요소들로 인증 모델을 나타낸다. 그리고 각 요소는 [그림 1]로 도식화하여 볼 수 있다.

- 정보 주체(인증신청자) : 하나 이상의 인증 프로토콜을 통해 신원을 인증 받는 정보 주체이다.
- 신뢰 당사자 : 거래를 처리하거나 정보의 접근을 허용하는 실체이다.
- 인증 서비스 : 하나 이상의 크리덴셜의 유효성을 결정하는 프로세스를 수행한다.
- 신뢰 승급 서비스 : 제공받고자 하는 거래의 위험 등급에 적절한 인증 방법을 선정하기 위한 프로세스를 수행한다.



〔그림 1〕 신뢰 승급이 가능한 인증 모델의 주요 요소

2.3. 신뢰 승급의 필요성

신뢰 승급을 하기 전에 인증 보증 등급이 결정되어야 한다. 인증 보증 등급은 위협 항목과 위험 항목의 영향을 받아 4단계의 인증 등급으로 나뉜다. 인증 보증 등급은 다음의 [표 2]과 같다.

〔표 2〕 인증 보증 등급〔1〕〔2〕〔4〕

	통제	설명
UAL-1	단일-요소 인증 또는 인증강도 1 이상	정보주체가 인증자를 통제하고 있다는 것을 낮은 수준으로 보증
UAL-2	이중-요소 인증 또는 인증강도 2 이상	정보주체가 인증자를 통제하고 있다는 것을 보통 수준으로 보증
UAL-3	삼중-요소 인증 또는 인증강도 3 이상	정보주체가 인증자를 통제하고 있다는 것을 높은 수준으로 보증
UAL-4	삼중-요소 인증 + 간섭 저항 하드웨어 모듈(TRM) 수준의 인증 또는 인증강도 4 이상	정보주체가 인증자를 통제하고 있다는 것을 매우 높은 수준으로 보증

신뢰 승급은 거래에 대한 위험 등급에 대응되는 추가 인증 방법으로 수행한다. 예를 들면, UAL-1의 인증 보증 등급에서 추가의 금융서비스를 해야 할 때, UAL-2 혹은 UAL-3, UAL-4로 인증해야한다.

2.4. 위협 항목에 대응되는 보증 수준

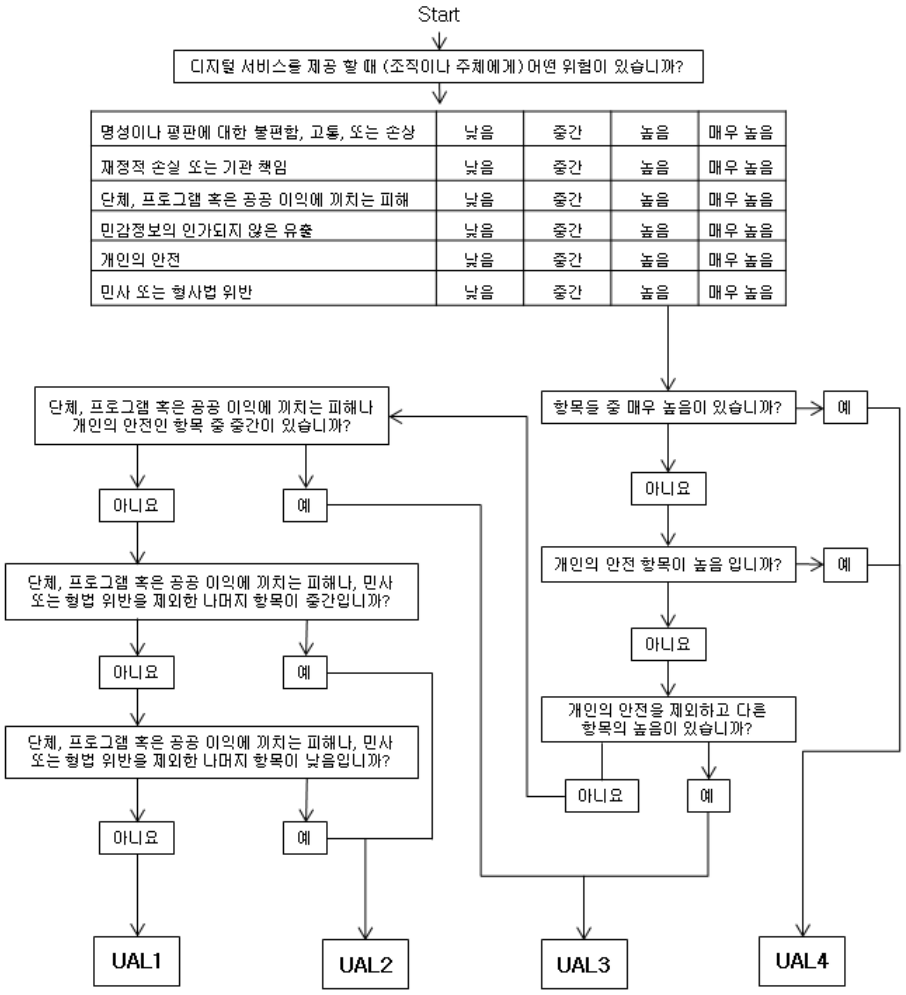
4단계의 인증 보증 등급은 다음의 위협 환경에 따라 분류된다. 다음의 [표 3]는 위협항목을 6가지로 나누어 보증 수준을 낮음부터 매우 높음까지 제시하였다. 그리고 [그림 2]는 위협항목을 적당한 보증 수준으로 선택할 수 있는지를 도식화하였다.

〔표 3〕 위협 항목에 대응되는 보증 수준[3]

위협 항목	보증 수준			
	1	2	3	4
지위 혹은 평판에 끼치는 불편, 고통 혹은 피해	낮음	중간	높음	매우 높음
재정적 손실 혹은 기관의 법적 책임	낮음	중간	높음	매우 높음
단체, 프로그램 혹은 공공 이익에 끼치는 피해	해당 없음	낮음	중간	매우 높음
민감 정보의 인가되지 않은 유출	해당 없음	중간	높음	매우 높음
개인의 안전	해당 없음	해당 없음	낮음-중간	높음-매우 높음
민사 혹은 형사 범죄	해당 없음	낮음	높음	매우 높음

2.5. 인증 보증 등급과 위험 등급

인증 보증 등급에 따라 이에 매칭되는 위험 등급을 제시한다. 이는 낮은 위험 등급, 보통 위험 등급, 높은



〔그림 2〕 위협에 따른 적당한 보증 수준 선택[3]

위험 등급, 매우 높은 위험 등급이 존재한다.

실제 금융서비스에서 각각의 위험 등급 별 서비스 항목은 아래 [표 5]와 같다. 위험등급이 높아질수록 강

〔표 4〕 위험 보증 등급과 위험 등급과의 매칭[4]

인증 등급	위험 등급	설명
UAL-1	TL-1	주장된 신원에 신뢰가 없음, 위험이 아주 낮음
UAL-2	TL-2	주장된 신원에 신뢰가 존재, 위험이 존재함
UAL-3	TL-3	주장된 신원에 높은 신뢰가 존재, 위험이 높음
UAL-4	TL-4	주장된 신원에 매우 높은 신뢰가 존재, 위험이 매우 높음

〔표 5〕 위험 등급 별 예시

위험 등급	예시
TL-1	계좌 조회
TL-2	계좌 이체(일정금액이하), 계좌 이체한도 축소, 공인인증서 내보내기&가져오기, 공인인증서 암호변경
TL-3	계좌 이체(일정금액이상), 계좌 발급, 거래계좌 해지, 계좌 비밀번호 변경(씨티은행), 계좌 연동 카드 발급, 공인인증서 갱신, 공인인증서 폐지
TL-4	계좌 이체한도 축소, 공인인증서 발급, 범용인증서 발급, OTP발급

도 높은 금융서비스가 해당한다. 각 위험 등급별 인증 수단은 [표 2]의 보증 등급 통제 항목에 따라야한다.

Ⅲ. 신뢰 승급 절차

3.1. 신뢰 승급이 필요하지 않은 경우 절차

신뢰 승급 절차는 신뢰 승급이 필요치 않은 경우와 신뢰 승급이 필요한 경우로 나눠서 볼 수 있다. 우선, 신뢰 승급이 필요치 않은 경우를 보면 요구하는 거래 수준에 현재 인증 등급이 적절한 경우로, 인증이 완료되면 서비스 이용이 가능하다. 이러한 신뢰 승급이 필요치 않은 인증 시나리오는 다음과 같다.

① 정보주체는 거래(예, 계좌 조회)를 신뢰 당사자에게 요구한다.
② 신뢰 당사자는 인가 서비스에게 해당 거래에 대응되는 인증 방법을 요청한다.
③ 인가 서비스는 해당 인증 방법을 전달한다.
④ 신뢰 당사자는 인증 서비스에게 정보 주체와 인증 방법(예, 이용자 ID + 패스워드) 으로 정보주체를 인증할 것을 요청한다.
⑤ 정보주체와 인증 서비스는 해당 인증 방법으로 인증을 수행한다.
⑥ 인증 서비스는 해당 인증 방법으로 정보주체가 인증이 완료되었음을 신뢰 당사자에게 통보한다.
⑦ 신뢰 당사자는 해당 거래에 대한 인증 방법에 의한 인증 성공을 인가 서비스에 통보한다.
⑧ 인가 서비스는 해당 거래에 대한 인증 방법을 확인하고, 정보주체가 인가되었음을 신뢰 당사자에게 통보한다.
⑨ 신뢰 당사자는 정보주체에게 정보주체에 의해 요청된 거래를 제공한다.

[그림 3]은 위의 인증 시나리오를 사용되고 있는 금융 서비스를 적용하여 도식화 하였다.

3.2. 신뢰 승급이 필요한 경우 절차

다음으로는 신뢰 승급이 필요한 인증 시나리오이다. 이미 한 번의 인증을 한 후, 추가로 금융 서비스를 이용하기 위해, 현재 인증된 인증 등급이 서비스를 이용하기 적절하지 못하여, 추가 인증을 진행하는 신뢰 승급 시나리오이다.

① ~ ⑨는 위의 시나리오와 같다.
⑩ 정보주체는 또 다른 거래(예, 자금 이체)를 신뢰 당사자에게 요구한다.
⑪ 신뢰 당사자는 인가 서비스에게 해당 거래에 대응되는 추가 인증 방법을 요청한다.
⑫ 인가서비스는 신뢰 승급 서비스에게 해당 거래에 대한 추가 인증 방법(예, 바이오 지문인증)을 요청한다.
⑬ 신뢰 인증 서비스는 인가 서비스에게 추가 인증 방법을 전달한다.
⑭ 인증 서비스는 신뢰 당사자에게 추가 인증 방법을 전달한다.
⑮ 신뢰 당사자는 인증 서비스에게 추가 인증으로 정보주체를 인증할 것을 요청한다.
⑯ 인증 신청자와 인증 서비스는 해당 인증 방법으로 인증을 수행한다.
⑰ 인증 서비스는 추가 인증 방법으로 정보주체가 인증이 완료되었음을 신뢰 당사자에게 통보한다.
⑱ 신뢰 당사자는 해당 거래에 대한 추가 인증 방법에 의한 인증 성공을 인가 서비스에 통보한다.
⑲ 인가 서비스는 해당 거래에 대한 추가 인증 방법을 확인하고, 정보주체가 인가되었음을 신뢰 당사자에게 통보한다.
⑳ 신뢰 당사자는 정보주체에게 요구되는 추가 거래를 제공한다.
⑩ ~ ⑳의 실제 활용 사례는 [그림 4]를 참조할 수 있다.

Ⅳ. 신뢰 승급이 가능한 보안 정책

신뢰 승급이 가능한 인증 보증 등급을 위한 보안 정책은 [표 6]와 같이 제시한다. 보안 정책은 초기 인증 등급을 기반으로 최종적으로 요구하는 인증 등급으로 승급하기 위한 필요한 정책으로, 신뢰 승급을 위한 추가 요구사항에 따라 분류하였다.

〔표 6〕 보안 방침〔5〕

위험 등급	초기 인증 등급	최종 인증 등급	추가 요구	정책 이름
저 등급	UAL-0	UAL-1	단일 요소 인증	P1
중	UAL-0	UAL-2	이중 요소 인증	P2

등급	UAL-1	UAL-2	UAL-1과 다른 추가 단일 요소 인증	P3
상 등급	UAL-0	UAL-3	삼중 요소 인증	P4
	UAL-1	UAL-3	UAL-1과 다른 추가 이중 요소 인증	P5
	UAL-2	UAL-3	UAL-2와 다른 추가 단일 요소 인증	P6
최상 등급	UAL-0	UAL-4	삼중 요소 인증과 TRM 수준의 인증 이용	P7
	UAL-1	UAL-4	UAL-1과 다른 추가 이중 요소 인증 (TRM 수준)	P8
	UAL-2	UAL-4	UAL-2와 다른 추가 단일 인증과 TRM 수준의 인증 이용	P9
	UAL-3	UAL-4	TRM 수준의 인증 추가	P10

Ⅴ. 금융 서비스에 활용 가능한 인증 수단

5.1. 인증 팩터별 엔트로피를 활용한 인증 강도 측정

엔트로피란 실제 키 값의 예측 가능성으로 정의된다. 인증 팩터별 인증 강도를 나눠서 위의 보증 등급을 구현하였고 다음의 방법으로 엔트로피를 구함을 알 수 있다. 엔트로피는 지식기반, 생체기반의 방법으로 구하는 방법이 있다.

5.1.1. 지식기반 인증 팩터

5.1.1.1. 패스워드

개인정보의 안전성 확보조치 기준(2011.9.30.,제정, 행정안전부 고시 제 2011-43호) 제5조(비밀번호 관리)에 근거하여 비밀번호 작성규칙에 따라 패스워드 길이를 규정한다. 이를 적용하여 엔트로피를 산정한다.

- 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 2종류 이상으로 구성한 경우
- 최소 8자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 3종류 이상으로 구성한 경우

식 (1)은 키 스페이스를 구하는 공식으로, n는 패스워드의 길이를 뜻하고, c는 Alphanumeric character로 A-Z, a-z와 0-9, 그리고 특수문자의 개수의 합인 94가 된다.[7]

$$k_p = c^n \tag{1}$$

식 (2)는 엔트로피를 구하는 공식이다.

$$H_{\max} = \log_2 k_p \tag{2}$$

예를 들면, 8자리의 패스워드의 키 스페이스는 $k_p = 94^8$가 되고, 이를 식 (2)에 대입하면 $\log 94^8 = \frac{\log 94^8}{\log 2} = 52.4367$가 된다. 패스워드는 대문자, 소문자, 숫자, 특수문자의 조합이 여러 개의 경우의 수가 있어서 이를 [표 7]로 정리하였다.

〔표 7〕 패스워드의 엔트로피

	패스워드 조합		키 스페이스	엔트로피
최소 8자리 이상	PW 1	대문자(또는 소문자) + 숫자 + 특수문자	68^8	48.6997
	PW 2	대문자 + 소문자 + 숫자	62^8	47.6336
	PW 3	대문자 + 소문자 + 특수문자	84^8	51.1385
	PW 4	대문자 + 소문자 + 숫자 + 특수문자	94^8	52.4367
최소 10자리 이상	PW 5	대문자 + 소문자	52^10	57.0044
	PW 6	대문자(또는 소문자) + 숫자	36^10	51.6993

	PW 7	대문자(또는 소문자) + 특수문자	58^10	58.5798
	PW 8	대문자(또는 소문자) + 숫자 + 특수문자	68^10	60.8746
	PW 9	대문자 + 소문자 + 숫자	62^10	59.5420
	PW 10	대문자 + 소문자 + 특수문자	84^10	63.9232
	PW 11	대문자 + 소문자 + 숫자 + 특수문자	94^10	64.5459

5.1.1.2. PIN

패스워드와 같은 방식으로 식 (1)과 식(2)를 활용하여 PIN 길에 따른 엔트로피를 산정한다. 단, 패스워드와 다르게 0~9의 범위를 가지므로 식 (1)의 c에 10을 대입한다. 예를 들면, 4자리의 핀의 키스페이스는 $k_p = 10^4$가 되고, 이를 식 (2)에 대입하면 $\log_2 10^4 = 13.2877$이 되고, 6자리의 PIN은 $\log_2 10^6 = 19.9316$이 된다.

5.1.2. 소지기반 인증 팩터

소지기반 인증 팩터의 엔트로피 계산은 키 스페이스와 식 (2)를 활용하여 엔트로피를 산정 할 수 있다.

〔표 8〕 소지 인증의 엔트로피

방식 설명		키 스페이스	엔트로피
OTP		10^6	19.9316
보안카드		10^2*35P2	16.8606
SMS	4자리	10^4	13.2877
	6자리	10^6	19.9316
공인인증서		2048bit(2^20)	20

5.1.3. 생체기반 인증 팩터

생체기반 인증 팩터의 엔트로피 계산은 FMR과 식 (4)를 참고하여 엔트로피 계산에 필요한 키 스페이스를 구하고, 식 (2)와 동일한 식 (5)를 활용하여 엔트로피를 산정 할 수 있다.

$$p(false\ match) = FMR(1) \tag{3}$$

$$k_b = 1/FMR(1) \tag{4}$$

$$H_{\max} = \log_2 k_b \tag{5}$$

다음의 [표 9]은 바이오 인증 방식을 FMR과 엔트로피를 계산한 수치를 표로 정리하였다.

〔표 9〕 바이오 인증의 엔트로피〔6〕〔8〕〔10〕〔11〕

방식 설명	FMR(%)	엔트로피
바이오 인증-얼굴	0.001	9.9658
바이오 인증-홍채	0.0001	13.2877
바이오 인증-지문	0.001	9.9658
바이오 인증-음성	0.01	6.6439
바이오 인증-정맥	0.0001	13.2877
바이오 인증-키스트로크(키스와이핑)	0.01	6.6439
바이오 인증-마우스움직임	0.43	1.2176

5.1.4. 엔트로피에 따른 인증 강도

엔트로피의 기준은 정책적으로 선정 가능하며, 지식, 소지, 바이오기반의 수단별로 상황이나 환경에 따라 영향을 받게 될 수 있으므로, 엔트로피의 강도 기준점을 다르게 잡아야한다고 본다. 따라서, 본 논문에서는 지식기반의 경우에는 20과 60을, 바이오기반의 경우에는 10으로, 소지기반의 경우에는 15로 엔트로피 값을 기준 삼았다. 지식기반의 경우는 상대적으로 길이가 짧은 PIN보다 패스워드가 강도가 높다고 산정하였다. 그렇다고 엔트로피의 기준점을 높게 지정 할 경우 PIN의 길이가 증가하여도 강도가 2로 바뀔 수 없기 때문에 PIN(6자리)를 기준으로 보고 20으로 기준점을 잡았다. 앞으로 PIN(8자리)가 나오게 되면 강도 2를 가질 수 있도록 가능성을 둔 것이다. 또한 패스워드의 경우 10자리 이상이며 조합이 대문자, 소문자, 숫자, 특수문자와 같이 4가지의 경우가 되면 엔트로피의 수치가 증가하게 되어 60 이상은 3의 강도를 가지게 된다. 생체기반의 경우는 안면과 지문이 9.9658이고, 홍채와 정맥이 13.2877이 계산되었다. 안면과 지문에 비해 홍채가 오인식률이 낮고 복제나 다른 위협에 비해 공격이 어

렵기 때문에 10으로 기준점을 잡았다. 마지막으로 소지기반에서는 OTP와 공인인증서는 15 이상의 엔트로피 값으로 강도가 높음을 알 수 있다.

〔표 10〕 인증 방식 별 인증 강도

방식 설명			엔트로피	인증 강도
PIN(4자리)			13.2877	1
PIN(6자리)			19.9319	1
패스워드(8자리)	PW 1	대문자(또는 소문자) + 숫자 + 특수문자	48.6997	2
	PW 2	대문자 + 소문자 + 숫자	47.6336	2
	PW 3	대문자 + 소문자 + 특수문자	51.1385	2
	PW 4	대문자 + 소문자 + 숫자 + 특수문자	52.4367	2
패스워드(10자리)	PW 5	대문자 + 소문자	57.0044	2
	PW 6	대문자(또는 소문자) + 숫자	51.6993	2
	PW 7	대문자(또는 소문자) + 특수문자	58.5798	2
	PW 8	대문자(또는 소문자) + 숫자 + 특수문자	60.8746	3
	PW 9	대문자 + 소문자 + 숫자	59.5420	2
	PW 10	대문자 + 소문자 + 특수문자	63.9232	3
	PW 11	대문자 + 소문자 + 숫자 + 특수문자	64.5459	3
바이오 인증-안면			9.9658	1
바이오 인증-홍채			13.2877	2
바이오 인증-지문			9.9658	1
바이오 인증-음성			6.6439	1
바이오 인증-정맥			13.2877	2
바이오 인증-키스트로크(키스와이핑)			6.6439	1
바이오 인증-마우스움직임			1.2176	1
OTP			19.9316	3
SMS		4자리	13.2877	2
		6자리	19.9316	3
공인인증서			20	3

5.2. 신뢰 승급에 적용 가능한 인증 수단

5.2.1. 다중 인증 요소의 강도

[표 2]의 인증 보증 등급의 통제 항목에 관련하여, 다중 인증인 경우는 아래의 5.2.2의 경우를 제외하고는 등급은 승급이 되지만, 강도는 승급이 되지 않는다. 다중 인증에서 조합되는 인증수단별 최고 강도의 +가 된다.

〔표 11〕 다중인증 요소의 강도 예시

	인증 수단 조합	
1	강도1 + 강도1	강도1+
2	강도1 + 강도1 + 강도1	강도1+
3	강도1 + 강도2	강도2+
4	강도1 + 강도1 + 강도2	강도2+
5	강도2 + 강도2	강도2+
6	강도1 + 강도3	강도3+
7	강도2 + 강도3	강도3+
8	강도1 + 강도2 + 강도3	강도3+
9	강도3 + 강도3	강도3+
10	강도3 + 강도4	강도4+
11	강도4 + 강도4	강도4+
12	강도4 + 강도4 + …	강도4+

예를 들면, [표 10]과 같이 강도1인 PIN과 강도2인 홍채를 이용하여 이중 인증을 하는 경우에는 강도1와 강도2를 합쳐도 2+의 강도를 가지게 되고 강도3로 승급을 하지 못한다.

5.2.2. 강도의 신뢰 승급

위의 다중인증 요소에 멀티모달의 개념을 적용하면, 등급뿐만 아니라 강도의 승급이 가능해진다. 멀티모달(Multi Modal)이란 하나의 특징이 아닌 두 개 이상의 특징을 결합하는 것으로, 두 가지 바이오 정보를 확인하여 본인을 식별하기 때문에 오인식률이 매우 낮아진다. 이를 활용하여 강도의 승급에 적용하였다.

강도의 경우 5.1.1고 같이 강도 n의 인증수단이 N개가 모여도 강도는 n+이상이 될 수 없다. 그러나 멀티모달의 개념으로 2개의 바이오기반의 인증이 포함되면 강도는 n+1로 승급이 가능해진다. 아래의 [표 12]는 신뢰 승급이 가능한 예시이다.

위의 [표 12]의 개념을 토대로 다음 [표 13]에서는 인증수단의 예시를 들어보았다.

〔표 12〕 인증수단 조합 별 승급 강도

	인증수단 조합	승급 강도
1	강도n + 강도n	강도n+
2	강도n + 강도n + …	강도n+
3	강도n + 강도n(바이오) + 강도n(바이오)	강도n+1
4	강도n + 강도n(바이오) + 강도n(바이오) + …	강도n+1+

〔표 13〕 인증수단 조합 별 승급 강도

	인증수단 조합 예시	승급 강도
1	지문(1) + PIN(1)	1+
2	지문(1) + 안면(1) + PIN(1)	2
3	PIN(1) + 정맥(2)	2+
4	정맥(2) + 홍채(2)	3
5	홍채(2) + OTP(3)	3+
6	지문(1) + 키스트로크(1) + OTP(3)	4
7	안면(1) + 키스트로크(1) + 패스워드(PW8(3))	4

5.2.3. 인증 수단 별 인증 강도의 예시

여러 금융서비스에 이용되는 인증 수단이 있다. 그 중에서 대표적으로 사용되는 인증 수단을 간추려 다음 [표 14]으로 나타내었다. 각 인증수단을 번호로 매핑하였고, 각 수단 별 인증 강도가 부여된다. 이 강도의 척도는 5.1절에서 구한 엔트로피와 NIST SP800-63, ITU-T X.1254 등의 문서를 분석하여 산정되었다.

〔표 14〕 인증 수단

인증 수단 번호	수단 설명	인증 유형	인증 강도
M1	PIN	지식	1
M2	패스워드(PW4)	지식	2
M3	공인인증서	소지	3
M4	OTP	소지	3
M5	바이오 인증-안면	바이오	1
M6	바이오 인증-지문	바이오	1
M7	바이오 인증-음성	바이오	1
M8	바이오 인증-홍채	바이오	2
M9	바이오 인증 - 키스트로크 (키스와이핑)	바이오	1
M10	PIN + 홍채	지식 + 바이오	2+
M11	OTP +공인인증서	지식 + 소지	3+
M12	키스트로크 (키스와이핑)+ 안면	바이오 + 바이오	2
M13	PIN+안면+ 공인인증서	지식 + 바이오 + 소지	3+

5.3. 인증 수단의 명시적 인증과 묵시적 인증

인증에는 명시적/묵시적 인증이 있다. 명시적 인증은 사용자가 신원을 증명할 것을 요구한 뒤 정보를 인지하여 인증하는 것을 의미한다.

묵시적 인증은 지속적으로 정보를 분석하여 사용자가 얼굴 촬영 등을 인지하지 못하는 상황에서 인증을 한다. [표 15]은 각 인증 수단 별 명시적 인증인지 묵시적 인증인지를 나타낸다.

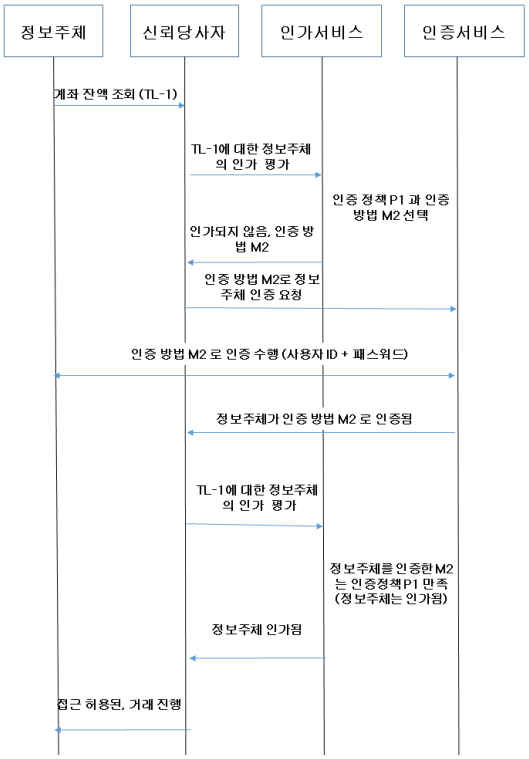
〔표 15〕 수단 별 명시적/묵시적 인증[9]

인증 수단	명시적/묵시적
비밀번호	명시적
토큰	명시적
얼굴&홍채	명시적/묵시적
지문	명시적
키스트로크 (키 스와이핑)	명시적/묵시적

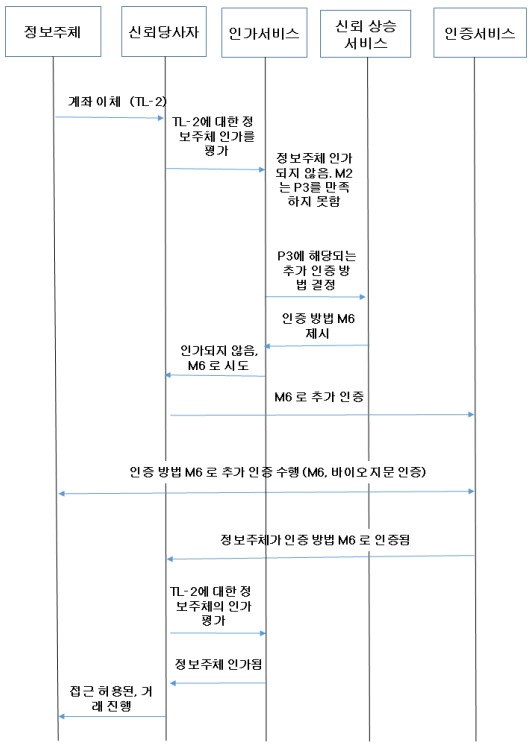
Ⅵ. 금융 서비스에 활용 가능한 인증 수단

본 논문에 제시한 인증 등급과 신뢰 승급 등급, 그리고 [표 6]의 보안정책 및 [표 14]의 인증수단을 이용하여 실제 사용되는 금융서비스가 어떻게 활용되어지는지 도식화하였다.

[표 5]에서 정의한 위험 수준이 TL-1인 은행 계좌 잔액을 확인하기 위한 흐름도의 예는 [그림 3]과 같다. 흐



〔그림 3〕 은행 계좌 잔액을 검사하기 위한 흐름도[5]



〔그림 4〕 은행 계좌 이체를 위한 신뢰 승급 흐름도[5]

름도에는 위에 제시된 [표 5]의 위험등급 TL-1, [표 6]의 인증 정책 P1과 [표 14]의 인증방법 M2가 사용된다. 이 활용 사례는 신뢰승급이 필요하지 않은 경우이다.

그리고, 신뢰 승급이 필요한 경우로는, [표 5]의 위험등급이 TL-2인 은행 계좌 이체를 하는 경우이다. [그림 3]과 같이 이전에 계좌의 잔액을 검사하기 위해 UAL-1인 M2로 인증되었다고 가정한다. 계좌 이체를 하기 위해서는 UAL-2로 신뢰 승급이 필요하다. 이 경우의 [표 5]의 인증 정책은 P3에 해당하고, [표 14]의 M5의 인증 수단으로 추가 인증을 한다. 흐름도는 [그림 4]와 같다.

Ⅶ. 결 론

본 논문에서는 금융권에서 인증 수단들을 인증 보증 등급으로 분류하고 신뢰 승급이 가능한 경우의 절차를 볼 수 있었다. 먼저 신뢰 승급이 가능한 모델을 알아보았다. 그 후 인증 보증 등급을 위협 사항과 고려하여 4단계로 분류하였고 위험 등급과 매핑하여 그에 따른 정책과 인증 수단을 적절하게 제시하였다. 그리고 엔트로피와 상황 기반에 따른 인증 강도를 각 인증 수단에 부여하였다.

현재의 경우 금융권에 많은 금융서비스를 제공하고 있지만, 제공하는 서비스의 보증 등급이 위험 등급이나 위협에 따른 요구하는 보증등급과 맞지 않는 경우, 제시한 신뢰 승급 방법을 활용해 추가 인증을 하여 보안성과 안정성을 높일 수 있다.

향후 사용자들은 더 간편하면서도 보안성이 높은 금융서비스를 제공받길 원할 것이다. 제공하는 금융 서비스의 보증 등급을 파악하고 추가 서비스를 이용 시 제시하는 신뢰 승급을 참고하여 적절한 인증 정책과 수단을 사용하면 적재적소에 더 안전한 인증과정을 거칠 것이라고 기대한다.

참 고 문 헌

[1] ISO/IEC 29115, Information technology -- Security techniques - Entity authentication assurance framework, 2013.

[2] UK CESG, Good Practice Guide No. 44

Authentication and Credentials for use with HMG Online Services, October 2014.

[3] DRAFT NIST Special Publication 800-63-3, Digital Identity Guidelines, 2017.6.

[4] ITU-T X.1254, Entity authentication assurance framework, 2013.

[5] OASIS trust-el-protocol-v1.0 “Authentication Step-Up Protocol and Metadata Version 1.0”Edited by Andrew Hughes, Shaheen Abdul Jabbar, Shaheen Abdul Jabbar, Abbie Barbir, Mary Ruddy. 24 May 2016. OASIS Committee Specification 01. Latest version: http://docs.oasis-open.org/trust-el/trust-el-protocol/v1.0/os/trust-el-protocol-v1.0-os.pdf

[6] Roman V.Yampolskiy, Venu Govindaraju, “Behavioural biometrics: a survey and classification”, International Journal of Biometrics (IJBM), 2008.

[7] Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, Darya Kurilova, Michelle L. Mazurek, William Melicher, Richard Shay, “Measuring Real-World Accuracies and Biases in Modeling Password Guessability”, USENIX Security Symposium, 2015.8

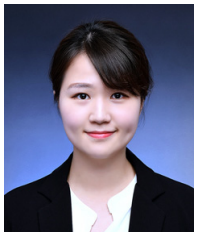
[8] NIST SP 800-76-2, Biometric Specifications for Personal Identity Verification, 2013.7

[9] Tobias Stockinger, “Implicit Authentication On Mobile Devices”, Media Informatics Advanced, Seminar on Ubiquitous Computing, 2011.

[10] Paulo Silva, “A new level of Biometric Technology Solutions”, Fujitsu, 2013

[11] Florian Schroff, Dmitry Kalenichenko, James Philbin, “FaceNet: A Unified Embedding for Face Recognition and Clustering”, 2015. 1.

〈저 자 소 개〉



김 지 혜 (Ji-Hye Kim)
학생회원

2016년 2월 : 순천향대학교 전기공학과 졸업
2016년 9월~현재 : 순천향대학교 융합서비스보안학과 석사 과정
관심분야 : 개인정보보호, 바이오인증, 개인정보 영향평가, 개인정보관리체계

사 경 진 (Kyeong-Jin Sa)
학생회원

2016년 2월 : 순천향대학교 전기공학과 졸업
2016년 3월~현재 : 순천향대학교 융합서비스보안학과 석사 과정
관심분야 : 개인정보보호, 바이오인증, IoT 보안, 악성코드

염 흥 열(Heung-Youl Youm)
종신회원

한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사 졸업
한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월 : 한국전자통신 연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
2011년 1월~12월 : 한국정보보호학회 회장(역), 명예회장(현)
2009년~2016년 11월 : ITU-T SG17 부의장
2016년 11월~현재 : ITU-T SG17 의장
2009년~현재 : ITU-T SG17 WP2/WP3 의장
2012년 6월~2015년 5월 : 정보보호포럼 의장
2016년 5월~현재 : 개인정보보호표준포럼 의장
관심분야 : 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜