TTA Technical Report

기술보고서

TTAR-xx.xxxx 제정일:2018년 12월 xx일

바이오인식으로 강화된 일회용 식별 인증 기술(기술보고서)

Disposable Identification Authentication Technology Enhanced by Biometrics (Technical Report)

TTA 한국정보통신기술협회
Telecommunications Technology Association

기술보고서 초안 검토 위원회 바이오인식 프로젝트그룹(PG505)

기술보고서안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	기술보고서번호
기술보고서(과제) 제안	강병오	코리아엑스퍼트(주)	부장		
	유인지	코리아엑스퍼트(주)	부장		
	이순주	코리아엑스퍼트(주)	과장		
	김선국	코리아엑스퍼트(주)	대리		
기술보고서 초안 작성자	이순주	코리아엑스퍼트(주)	과장		
사무국 담당	김재웅	TTA	단장		
	문서연	TTA	전임		

본 기술보고서 발간 이전에 접수된 지식재산권 확약서 정보는 본 기술보고서의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 기술보고서와 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.12

서 문

1 기술보고서의 목적

끊임없이 발생하는 사용자 인증 관련 보안 이슈, 공인인증서 의무화 폐지와 같은 법제도 변화, 핀테크 활성화 및 모바일 중심의 서비스 전환에 따라 다양한 인증기술이 이슈화 되고 있다. 이 중 최근 소개되고 있는 인증 기술, 서비스 중 일회용 식별자 기반 인증이 주목받고 있다. 해당 방식은 고정된 아이디로 인한 사용자 인증의 근본적인 문제를 해결하고자 고정되지 않은 일회용 식별자를 인증에 활용하는 방식이다.
고정되지 않은 정보로 사용자를 식별함에 따라 아이디, 비밀번호, 2차 인증 등의 다양한 인증수단으로 활용할 수 있고, 바이오인식과 연계하여 보다 강화된 보안을 기반으로 사용자 인증에 활용될 수 있다.
본 기술보고서는 일회용 식별자 기반 인증 기술에 대해서 기술하고, 바이오인식으로 일회용 식별자 기반 인증을 강화하는 방안 등에 대해서 기술한다.
이를 통해 일회용 식별자 기반 인증에 대한 이해를 돕고, 향후 표준으로 활용하기 위한 기술 정보 제공을 목적으로 한다.

2 주요 내용 요약

일회용 식별자는 고정된 아이디 자체의 유출, 해킹의 위험요소를 제거하고, 아이디/비밀번호 암기 및 분실로 인한 사용자의 불편함을 해소할 수 있는 방식이다.
본 기술보고서는 사용자 인증 분야에서 일회용 식별자의 필요성을 기술하고, 이러한 필요성을 만족시킬 수 있는 일회용 식별 기술에 대해 설명한다. 또한 바이오인식 기술로 일회용 식별자 기반 인증의 보안성을 높일 수 있는 방안, 기대효과 등에 대해서 기술한다.

3 인용 기술보고서와의 비교

- 해당 사항 없음

Preface

1 Purpose

Various authentication technologies have become an issue due to the ever-increasing security issues related to user authentication, changes in legal systems such as the abolition of mandatory accredited certificate, the activation of Fin-Tech and mobile-centric switching services.

Among these, recently introduced authentication technologies and services based on disposable identifier are receiving spotlight. This is the way to use non-fixed disposable identifier for authentication to solve the fundamental problem of user authentication caused by fixed IDs.

By identifying users with non-fixed information, they can be used as various authentication methods such as ID, password, and secondary authentication, and are provided with more enhanced services in conjunction with biometric.

This technical report describes the technology for authentication based on disposable Identification, and explains how to enhance authentication based on disposable Identifier by utilizing biometric.

The purpose of this description is to facilitate understanding of disposable identifier-based authentication and to provide technical information for use as a standard in the future.

2 Summary

Despite the emergence of various user authentication technologies, most authentication makes users uncomfortable by applying additional authentication such as SMS, ARS, and OTP to prevent the leakage of fixed IDs, and places a cost burden on businesses

Disposable identifier are a way to eliminate the risk of identify leakage, hacking, and to reliever user inconvenience due to the memory and loss of ID/password.

This technical report describes the need for disposable identifier in the field of user authentication and explains the disposable identification technology that might meet these needs.

It also describes how biometric technologies can increase the security of disposable identification-based authentication, and the expected effects, etc.

3 Relationship to Reference Standards

-None

목 차

바이오인식으로 강화된 일회용 식별 인증 기술 (Disposable Identification Authentication Technology Enhanced by Biometrics)

1 적용 범위

본 기술보고서는 고정되지 않은 일회용 랜덤 코드로 사용자를 식별할 수 있는 일회용 식별자를 활용한 인증에 대한 사항을 기술한다. 일회용 식별자의 필요성, 일회용 식별자 활용 방법, 실제 서비스 사례, 적용 시 전제사항 등과 관련된 내용을 기술한다.

2 인용 표준

- 해당 사항 없음

3 용어 정의

3.1 일회용 식별자 (One Time Identifier)

일회용 식별자는 사용자를 식별할 수 있는 코드를 고정되지 않은 일회용 랜덤코드를 활용한 방식을 의미한다.

3.1 랜덤코드 (Random Code)

일회용 식별자를 활용해 사용자 인증 시 사용자가 확인하여 입력하는 일회용 코드값을 의미한다.

3.3 Credential

일회용 식별자를 이용하는 서비스 등록 시 사용자 구분을 위해 고객사 응용시스템에 요청하는 최소한의 정보를 의미한다. (예 : 사용자 아이디, 이름, 전화번호 등)

3.4 Seed

사용자별 중복되지 않고 Unique한 일회용 식별자를 생성하기 위해 사용되는 정보를 의미한다. 서비스 등록 시 획득한 사용자별 Credential 정보와 일회용 식별자 생성 알고리즘 등이 Seed 정보로 구성된다.

3.5 일회용식별자 토큰

일회용 식별자를 생성하는 매체를 의미한다. 일회용 식별자는 모바일, 태블릿, 스마트카드 등 다양한 매체를 통해 생성, 제공될 수 있다. 이는 사용자가 직접입력 할 수 있도록 문자로 형상화 되는 형태와, 일회용 식별자 생성 기술이 매체에 내장되어 기술적으로 활용되는 형태 등 다양하게 활용될 수 있다.

3.6 Multi Factor Authentication (다중 요소 인증)

2가지 이상의 인증 방법을 조합하여 보안성을 높이는 인증방식을 의미한다. 인증은 자신이 알고 있는 것(what you know, 예 : 비밀번호, PIN 등), 자신이 소유한 것(what you have, 예 : 토큰, 스마트카드 등) 자신 그 자체(what you are, 예 : 지문, 홍채, 걸음걸이 등의 바이오, 행동정보) 이다. 이들 중 하나의 요소만 이용하는 단일 인증은 보안에 취약하기 때문에 서로 다른 2개 이상의 인증을 조합한 방식이 다중 요소 인증방식이다. 예를 들어 스마트폰앱에서 제공되는 일회용 식별자와 바이오인식 기반 인증을 조합하여 인증 시 Multi Factor Authentication을 만족하며 보안성을 높일 수 있다.

3.7 인증서버

일회용 식별자 인증요청에 대한 검증 기능을 수행하는 서버를 의미한다.

3.8 UTC

UTC(Universal Time Coordinated, 협정세계시)는 전 세계에서 공통으로 사용하고 있는 국제 표준시를 의미한다. 일회용 식별자는 UTC를 기반으로 하여 국내뿐만 아니라 전세계 어느 곳에서든 동일하게 사용할 수 있도록 한다.

3.9 시간동기화 방식

시간동기화 방식은 서버와 일회용식별자 토큰 간에 동기화된 시각 정보를 기준으로, 특정 시간마다 변하는 코드를 생성하는 방식을 의미한다. 이 방식은 사용자의 인증요청과 상관없이 특정 시간 간격마다 매번 코드가 바뀌므로, 공격자가 해킹에 사용할 수 있는 코드를 얻어내기 어렵다.

3.10 Brute Force Attack

사용자 아이디, 비밀번호를 알아내기 위해 조합 가능한 모든 경우의 수를 무차별적으로 대입해 보는 코드 또는 암호 해독 목적의 공격 방식이다. 우리말로는 보통 무차별 대입 공격이라 칭한다. 대부분의 암호화 방식은 이론적으로 무차별 대입 공격에 안전하지 못하며, 충분한 시간이 존재한다면 암호화된 정보는 해독 가능하다. Brute Force Attack은 암호 체계를 적용하고 있는 대부분의 리소스를 대상으로 한다.

3.11 Salt

가변적이지 못한 고정된 Hash값의 단점을 보완하기 위해 Hash값을 가변적으로 만들어 주는 추가 문자열을 의미한다.

4 약어

AES Advanced Encryption Standard
API Application Programming Interface
FIDO Fast Identity Online
RFC Request for Comments
SHA Secure Hash Algorithm
SSL Secure Socket Layer
TLS Transport Layer Security
UTC Universal Time Coordinated

5 일회용 식별자 기본개념

5.1 일회용 식별자 매커니즘

일회용 식별자(One Time Identifier)는 매번 다른 일회용 랜덤코드로 사용자를 인증하는 방식을 의미한다. 아이디는 'Identity'의 사전적 의미대로 신원을 식별할 수 있는 수단이여야 하기 때문에, 사용자간 동일한 시점에 고유한 값이 부여되어야 한다. 일회용 식별자는 일회성 랜덤코드로 제공되고, 현재 사용하는 랜덤코드로 다음번에 사용할 랜덤코드를 유추할 수 없도록 예측 불가한 패턴으로 발생하게 된다.
일회용 식별자 기반의 인증 시, 사용자는 고정된 아이디를 암기할 필요 없고, 분실을 우려해 메모를 해둘 필요도 없으며, 유효시간 내 1회만 사용 가능하기 때문에 유출 및 해킹 시에도 염려할 필요가 없다.

5.2 일회용 식별자 생성

5.2.1 연계정보

일회용 식별자는 시각정보를 활용한 시간 동기화 방식으로 연계정보를 사용한다. 시각정보 기반의 연계정보는 특정한 시간 동안만 유효하여야 하며, 일회용 식별자 생성기와 인증서버에서 동일한 정보를 생성할 수 있어야 한다. 예를 들어 은행 인터넷뱅킹 서비스 영역에서 연계정보와 일회용 식별자는 30~60초 이내에서만 유효하도록 하는 등의 시간적 제한이 필요하다.
일회용 식별자의 시각은 UTC(Coordinated Universal Time, 국제표준시)를 기준으로 하여 지리적 요소에 제약 없이 해외 어디에서든 국내와 동일하게 사용 가능하도록 한다.

5.2.2 일회용 식별자 생성 알고리즘

HMAC-SHA1 알고리즘이 적용된 RFC4226 HOTP와 시간동기화 방식의 RFC6238 TOTP 등의 국내외 표준 알고리즘을 적용한다. 이를 기반으로 수학적 알고리즘을 활용한 복원

불가 일방향 유일코드 변환기를 추가 반영하여 사용자별 중복되지 않는 유일한 랜덤코드, 즉 일회용 식별자를 생성하도록 한다.
또한 관리자는 표현 문자셋, 길이, 시간 등의 정보를 유연하게 변경 할 수 있도록 한다.

5.3 일회용 식별자 토큰

5.3.1 소프트웨어 방식

소프트웨어 방식은 일회용 식별자 생성 토큰이 사용자가 소지하고 있는 스마트폰, 태블릿PC 등에 내장된 방식을 의미한다. 소프트웨어 방식은 전용 하드웨어 토큰형 및 카드형과는 다르게 소프트웨어 모듈 형태로 구현되며, 일반적으로 스마트폰앱, USIM 스마트카드에 내장되는 방식이다.
별도의 기기를 소지하지 않고 사용자가 소지한 스마트폰을 통해 일회용 식별자 기반 랜덤코드를 확인할 수 있어 편리하게 사용할 수 있다는 특징이 있다.

5.3.2 하드웨어 방식

하드웨어 방식은 토큰형과 카드형으로 나눌 수 있다. 토큰형 방식은 일회용 식별자를 생성할 수 있는 연산 기능, 암호 알고리즘 등이 토큰에 내장되어 있는 하드웨어 매체이다. 카드형 토큰은 IC 카드 내에 일회용 식별자 생성 모듈이 내장되어 있으며 디스플레이 창과 일회용 식별자 생성 버튼이 부착되어 있어 휴대하기 간편하다는 특징이 있다.
또한 보안을 위해 일회용 식별자 생성 알고리즘과 NFC기능이 탑재된 스마트카드와 스마트폰을 태핑하여 등록한 사용자임을 확인한 후 일회용 식별자를 생성하고, 스마트폰앱을 통해 랜덤코드를 디스플레이하는 방식도 응용 가능한 방식이다.

5.4 일회용 식별자 설정

일회용 식별자는 사용 가능한 유효시간을 설정해야 하며, 이는 적용 서비스의 특성에 따라 조정하여 설정하도록 한다. 더불어 유효시간 사용 횟수는 1회 사용을 원칙으로 한다. 단 일회용 식별자를 사용하는 서비스의 용도, 예외처리 적용여부에 따라 유효시간 내 재사용 가능여부는 서비스 운영기관과 논의하여 설정할 수 있도록 한다.
일회용 식별자의 자리 수 또한 서비스 운영기관과 논의하여 설정할 수 있다. 자리수는 사용 편의성 및 보안의 적정성을 위해 4~8자리를 권고한다.
일회용 식별자는 코드 조합의 다양성을 제공한다. 문자열의 조합은 82개 문자 (숫자, 영어 대/소문자, 특수문자)를 활용하여 제약 없이 조합할 수 있다. 숫자로만 구성하는 경우 입력이 편리하지만 타인에게 노출되기도 쉬워, 보안이 강조되는 서비스는 숫자와 문자를 혼합하여 구성할 경우 노출에도 안전할 수 있다. 서비스의 특성, 보안의 중요도에 따라 일회용 식별자의 설정을 조정할 수 있어야 한다.

(그림 5-1) 다양한 조합의 일회용 식별자

5.5 일회용 식별자 사용

5.5.1 등록

일회용 식별자 사용을 위해서는 최초에 등록 과정을 필요로 한다. 사용자 구분을 위해 이용기관 응용시스템으로부터 최소한의 정보를 전달 받는 과정이다.

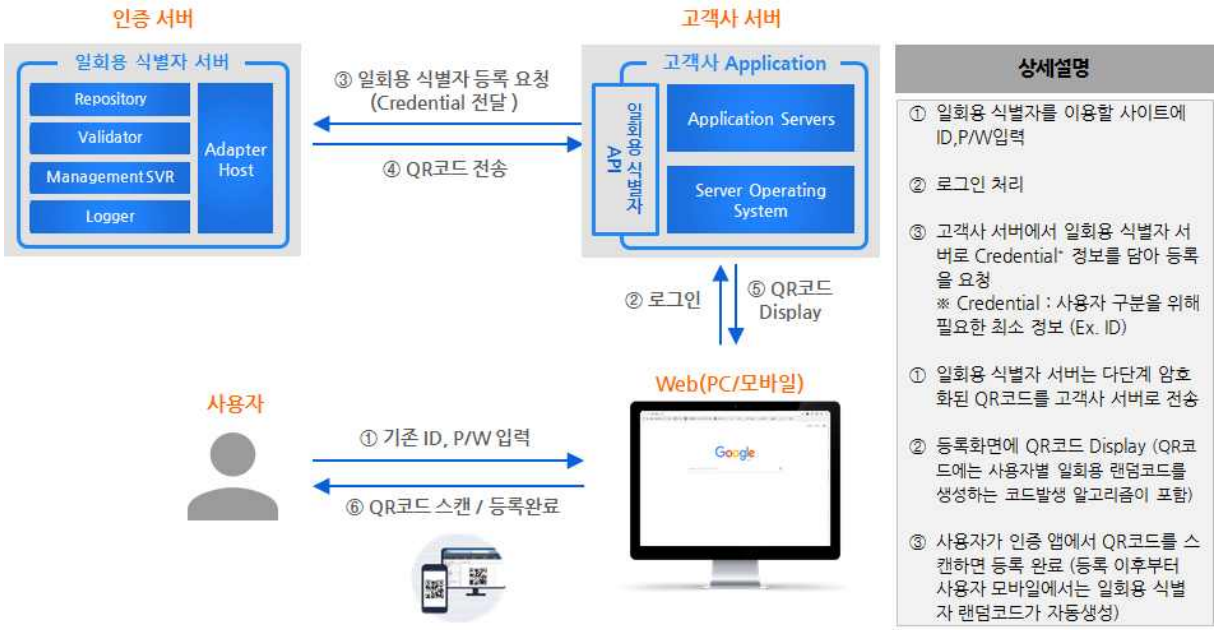
스마트폰앱 방식을 예로 들면 인증서버와 사용자 스마트폰앱에 동일한 일회용 식별자를 생성해내는 알고리즘을 탑재해야 하는데, 알고리즘을 전달하는 용도로는 QR코드, SMS, 이메일 등을 활용할 수 있다.

스마트폰앱 기반 일회용 식별자 인증서비스의 QR코드 활용 예시로 살펴보면 다음과 같다. 기존 아이디, 비밀번호로 시스템에 로그인하여 기존 어플리케이션에서 일회용 식별자 인증서버로 Credential 정보를 담아 일회용 식별자 등록 요청을 보낸다. 등록 요청을 받은 인증서버는 Credential 정보를 받고, 다단계 암호화된 QR코드를 어플리케이션 서버로 전송한다. 사용자가 스마트폰의 인증앱을 통해 화면에 Display된 QR코드를 스캔하면, 인증서버와 스마트폰앱에서 동일한 일회용 식별자를 생성해낼 수 있는 매칭 과정이 완료된다.

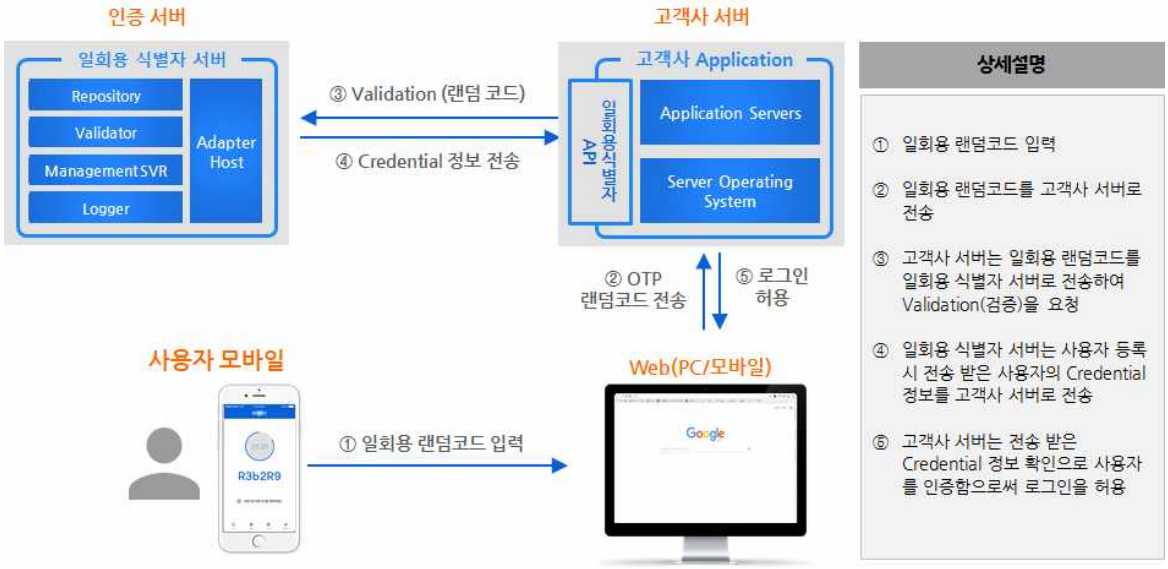
5.5.2 인증

사용자가 입력한 일회용 식별자는 어플리케이션 서버를 통해 인증서버로 전달되며, 메모리 및 hash key 값을 해싱하여 해당 사용자의 Credential을 찾아 어플리케이션 서버로 return하게 된다.

인증 시 사용자가 일회용 식별자를 직접 입력할 수도 있지만 사용 편의성을 고려해 사용자 환경(PC, 모바일, 태블릿)에 따라 인증 방식을 달리할 수 있다. PC환경에서도 일회용 식별자를 직접 입력하지 않고 QR코드를 스캔하는 방식, 모바일 환경에서 자동로그인 하는 방식 등 다양한 방식을 제공할 수 있어야 한다.



(그림 5-2) 일회용 식별자 기반 서비스 등록절차



(그림 5-3) 일회용 식별자 기반 서비스 인증절차

5.6 일회용 식별자 활용 방안

일회용 식별자는 사전 인증, 사용자 인증, 추가 인증 등 모든 인증 영역에 활용될 수 있다. 일회용 식별자 자체가 사용자별 중복되지 않는 랜덤코드로 사용자를 식별할 수 있어 사용자의 Identity를 확인할 수 있는 역할을 한다. 기존의 고정된 아이디, 비밀번호를 대신할 수 있다. OTP, ARS, SMS와 같은 2차 인증 수단으로 적용할 경우, 2차 인증에 앞서 사용한 아이디, 비밀번호로 사용자 식별을 선행하고, 일회용 식별자로 다시 한번 사용자를 식별하게 된다. 사용자를 이중 인증함으로써 보안의 강도를 높일 수 있다. 기존 2차 인증 방식은 그 자체만으로는 사용자 식별이 불가능하다.

(그림 5-4) 일회용 식별자 활용 방안

뿐만 아니라 아이디를 보호하는 역할의 사전인증으로도 활용 할 수 있다. 보통 로그인 시 보안강화를 위해 아이디, 비밀번호 입력 후 추가인증을 후속절차로 진행하는 것이 일반적이다. 하지만 이와 같은 경우 Brute Force Attack (무작위 대입 공격)에 노출 시 아이디, 비밀번호 탈취, 해킹에 속수무책이다. 이러한 경우 일회용 식별자로 사전인증을 통과한 사람에 한하여 아이디, 비밀번호를 입력할 수 있는 기회를 주는 방식이다.
일회용 식별자는 온라인뿐만 아니라 오프라인에서도 효과적으로 활용할 수 있다. 오프라인 장소 출입 허가, 기기간의 무선통신상 데이터 전송 분야 등에서 활용함으로써, On-Off Line 연계가 가능하도록 확장할 수 있다.

6 일회용 식별자 활용 사례

6.1 아이디

A공공기관은 대국민이 이용하는 재단 대표 홈페이지에 일회용 식별자를 적용했다. 기존 사용자의 아이디, 비밀번호 암기 필요, 분실 또는 재발급으로 인한 불편함으로 고객의 서비스 이탈이 발생하기도 했다. 해킹 및 유출사고에 대한 대비책으로 일회용 식별자를 활용했다. 기존 또한 아이디, 비밀번호 방식과 일회용 식별자 기반 인증 방식 2가지를 동시에 제공하여, 사용자 원하는 방식을 선택할 수 있도록 한 사례이다.

6.2 추가인증

개인정보를 취급하는 다수의 기업, 기관에서는 일회용 식별자 기반 인증을 추가인증 방식으로 활용하였다. 보험사의 설계사 영업지원 시스템, 서버접근 제어, 문서중앙화/파일서버/무선인증/NAC 등의 보안솔루션에 연계하여, 일회용 식별자를 OTP, SMS, 또는 인증서 대체 용도로 적용하였다.

(그림 6-1) 일회용 식별자 활용사례 - 로그인 시 아이디 용도

서비스 운영기관에서는 개인정보를 취급하는 주요 시스템 접근 시 2차 인증을 필요로 하는 정부 가이드를 준수하면서, 단순한 2차 인증이 아닌, 사용자 이중 인증을 실현한 사례로 타 2차 인증 솔루션대비 보안 측면의 만족도가 높다.

(그림 6-2) 일회용 식별자 활용사례 - 추가인증 용도

7. 바이오인식 연계 방안

최근 사용자 편의성은 향상시키면서 높은 수준을 보안을 유지할 수 있게 하는 다양한 인증방식이 시장에 소개되고 있는데, 그 중 바이오정보, 일회용 식별자는 모두 사용자를 구분할 수 있는 방식이기 때문에 상호 보완적인 역할로 연계할 수 있다.

일회용 식별자의 보안조치를 위해 바이오인식을 활용할 수 있고, Multi Factor 인증 만족을 위해 2가지 방식을 접목해 사용할 수 있다.

또한 바이오인식의 제약사항으로 인한 이슈를 해결하는 용도로 일회용 식별자를 활용하는 방안도 있어, 다양한 경우의 연계 활용이 가능하다.

7.1 일회용식별자 보안을 위한 바이오인식 활용

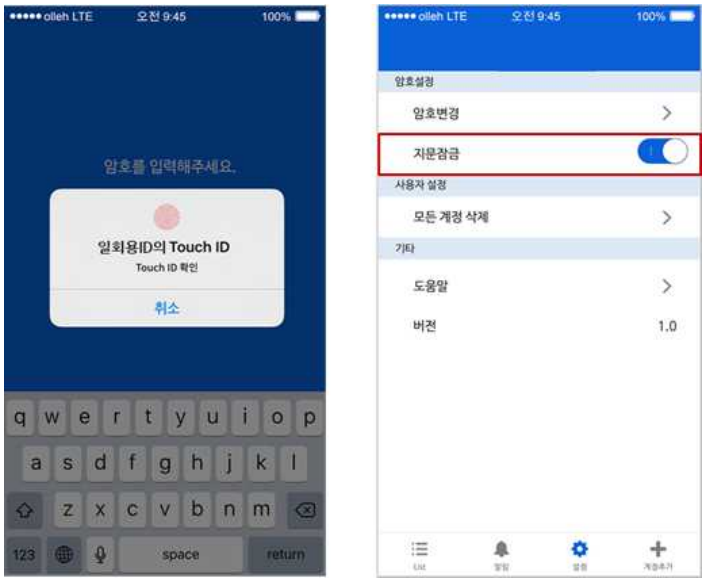
사용자의 특정 기기에서 생성되는 일회용 식별자는 랜덤코드 유출에 대비한 잠금 기능으로 보안성을 높일 수 있다.

스마트폰앱 기반의 일회용 식별자의 경우, 휴대폰 자체에서 제공하는 바이오인식 기능을 활용할 수 있다. 스마트폰앱 실행 시, 또는 앱 실행 후 랜덤코드 확인 직전에 지문인식, 홍채인식, 안면인식 등의 바이오인식을 통해 사용자를 확인한 후, 확인된 사용자에 한하여 앱에 접근, 랜덤코드를 확인할 수 있도록 하는 방식이다.

7.2 바이오인식과의 연계

바이오인식은 개인의 바이오정보를 인증에 활용한다는 특징으로 보다 편리한 인증을 가능하게 해주는 장점이 있다. 하지만 여러 가지 제약사항이 존재한다.

개인의 바이오정보를 인증에 활용하는 것에 대한 사용자 거부감, 사용자의 휴대기기에



(그림 7-1) 바이오인식을 연계한 일회용 식별자 보호 방안

바이오인식 기능이 탑재되어 있지 않은 경우 사용 불가, 등록된 바이오정보가 훼손 된 경우 인식의 어려움, 기타 상황으로 인한 처리 오류가 발생하거나 처리가 불가능한 경우에 대비하여야 한다.

이에 대한 대비책으로 바이오인식 방식과 일회용 식별자에 제공함으로서 서비스 및 업무 시스템 이용의 연속성을 보장하고, 다양한 환경의 사용자층을 커버할 수 있다.

또한 바이오인식은 생체기반(특성기반)의 인증방식, 일회용식별자는 소지 기반 인증방식으로, 2가지 방식을 결합하여 사용할 경우 Multi Factor 인증을 만족할 수 있다.

부 록 Ⅰ-1

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

지식재산권 확약서 정보

- 해당사항없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 기술보고서가 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

시험인증 관련 사항

- 해당사항없음

부 록 Ⅰ-3

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

본 기술보고서의 연계(family) 표준

- 해당사항없음

부 록 Ⅰ-4

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

참고 문헌

[1] TTAK.IT-X1088, "바이오 인식 정보에 기반한 전자서명 키생성 프레임워크", 2008
[2] TAK.KO-12.0098, "One-Time 템플릿 기반의 바이오 인증 프레임워크", 2008
[2] TTAK.KO-12.0302, "금융보안을 위한 바이오인식 운영 지침", 2016

부 록 Ⅰ-5

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

영문기술보고서 해설서

- 해당사항없음

부 록 Ⅰ-6

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

기술보고서의 이력

판수	채택일	기술보고서번호	내용	담당 위원회
제1판			바이오인식으로 강화된 일회용 식별 인증 기술 (기술보고서)	PG505