

# Introduction of eWBM FIDO2 Security key with Microsoft Azure AD

파이도2를 이용한 쉽고 간편하고 높은 보안의 클라우드 로그인 방법

Sales & Marketing

eWBM



Copyright © eWBM Co., Ltd. All rights reserved.

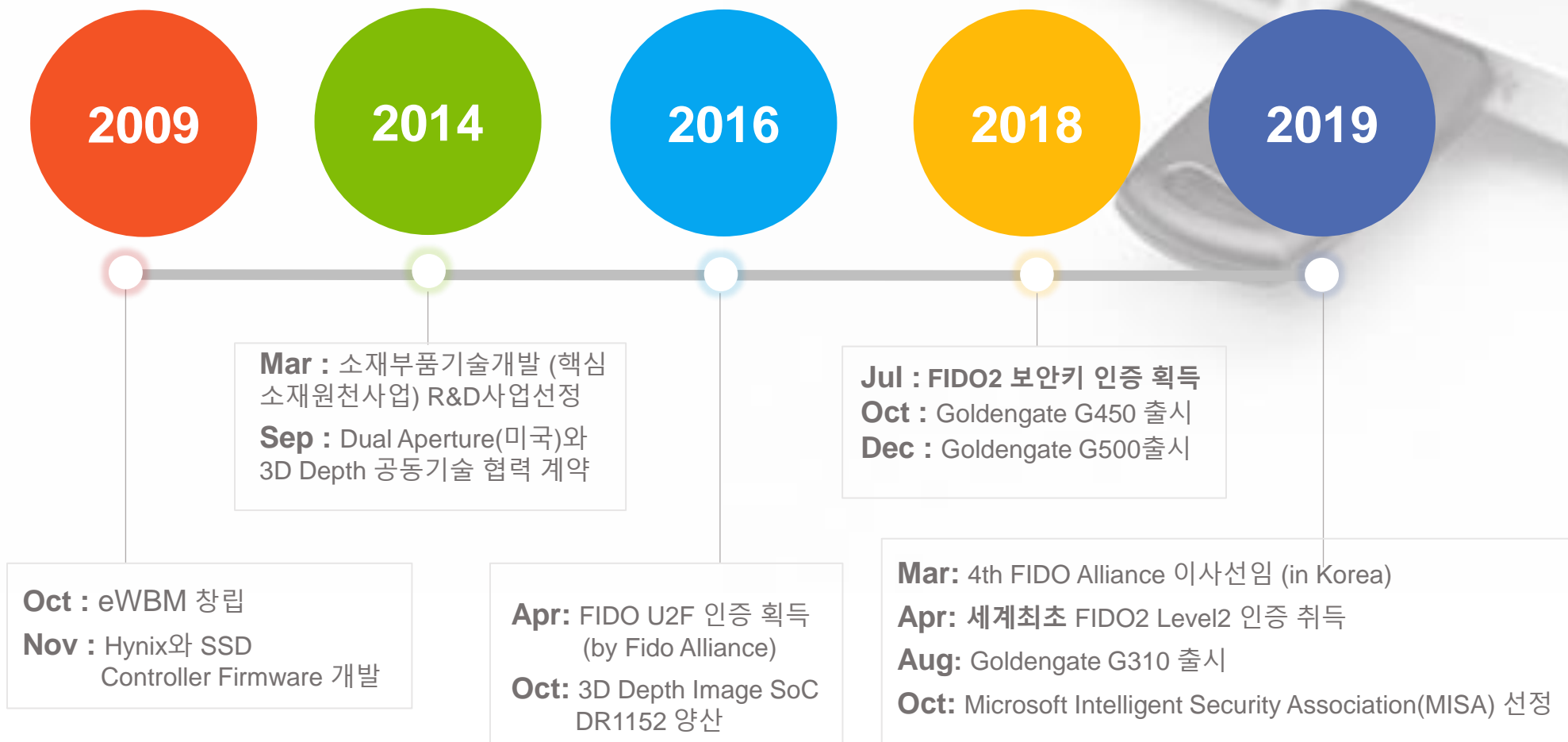


**Founded on** 2009년 10월 15일

**CEO:** Stephen Oh, Ph.D.

**R&D Center:** 서울특별시 강남구 테헤란로20길 9, 14층 06236 (역삼동 동궁빌딩)

**US Office:** 2100 Alamo Rd Suite T, Richardson, TX

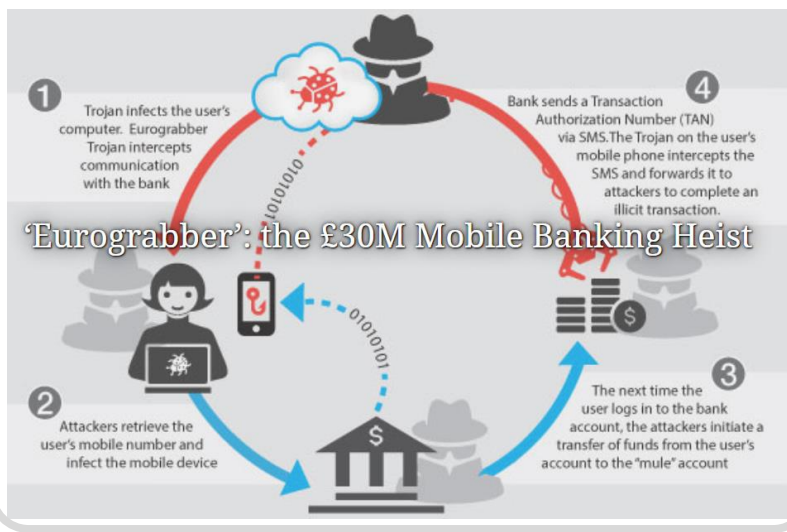


# 인증보안 취약성 및 피해 사례 증가

## 재택근무시 기업 해킹 위험성 증가



## OTP 사용시 2차 해킹 사례



## 공시생, 인사혁신처 PC 9시간 헤집고 다녔다

김충형 기자 김정환 기자

승인 2020.01.14 | 입력 : 2016.04.07 03:00

"클라우드 해킹" 논란... "아이디·패스워드 '다르게'... 인증은 2단계로 철저히"

클라우드 서버에 휴대전화 속 자료를 저장한 후 인터넷에 접속하기만 하면 이용할 수 있는 서비스다. 보안 전문가들은 이번 해킹 사건이 클라우드 자체가 직접 해킹당했다기보다는, 클라우드 아이디와 패스워드가 유출되면서 발생한 것으로 보고 있다.

- 정부청사를 자기 안방처럼

## 재택근무 증가에 해킹 피해도 21% 급증

승인 2020.04.06 11:11 | PC를 자기 PC처럼

SK인포섹은 6일 올해 1분기 자사 보안관제센터인 '시큐디움 센터'에서 탐지한 사이버 공격 건수가 총 174만7000여건에 달한다고 밝혔다.

이는 월평균 58만건 수준으로 지난해 1분기 월별 평균치인 48만건보다 21% 증가했다.

## "재택·원격근무 시 해킹 위험"... 정부 '정보유출 방지를 위한 실천 수칙' 권고

승인 2020.03.30 16:59 |

최근 '코로나19' 이슈를 악용하여 사용 중인 문자가 지속적으로 유포되고 있다. 관리 체계를 노린 랜섬웨어 공격 피해가하고 있는 상황이다.

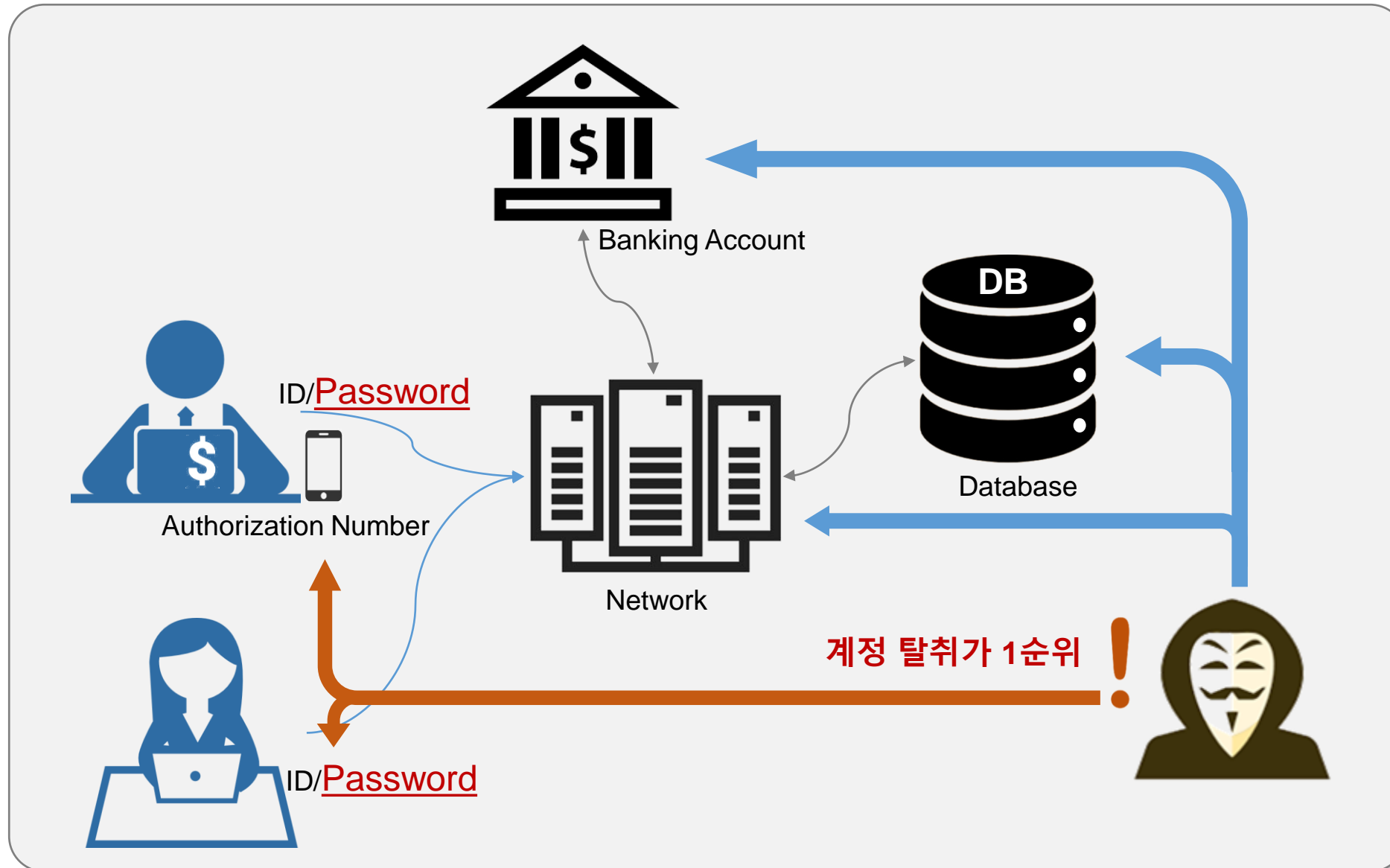
## 미래에셋, 피싱 피해로 60억원 날려

입력 2020.03.26 18:23 | 수정 2020.03.26 18:28

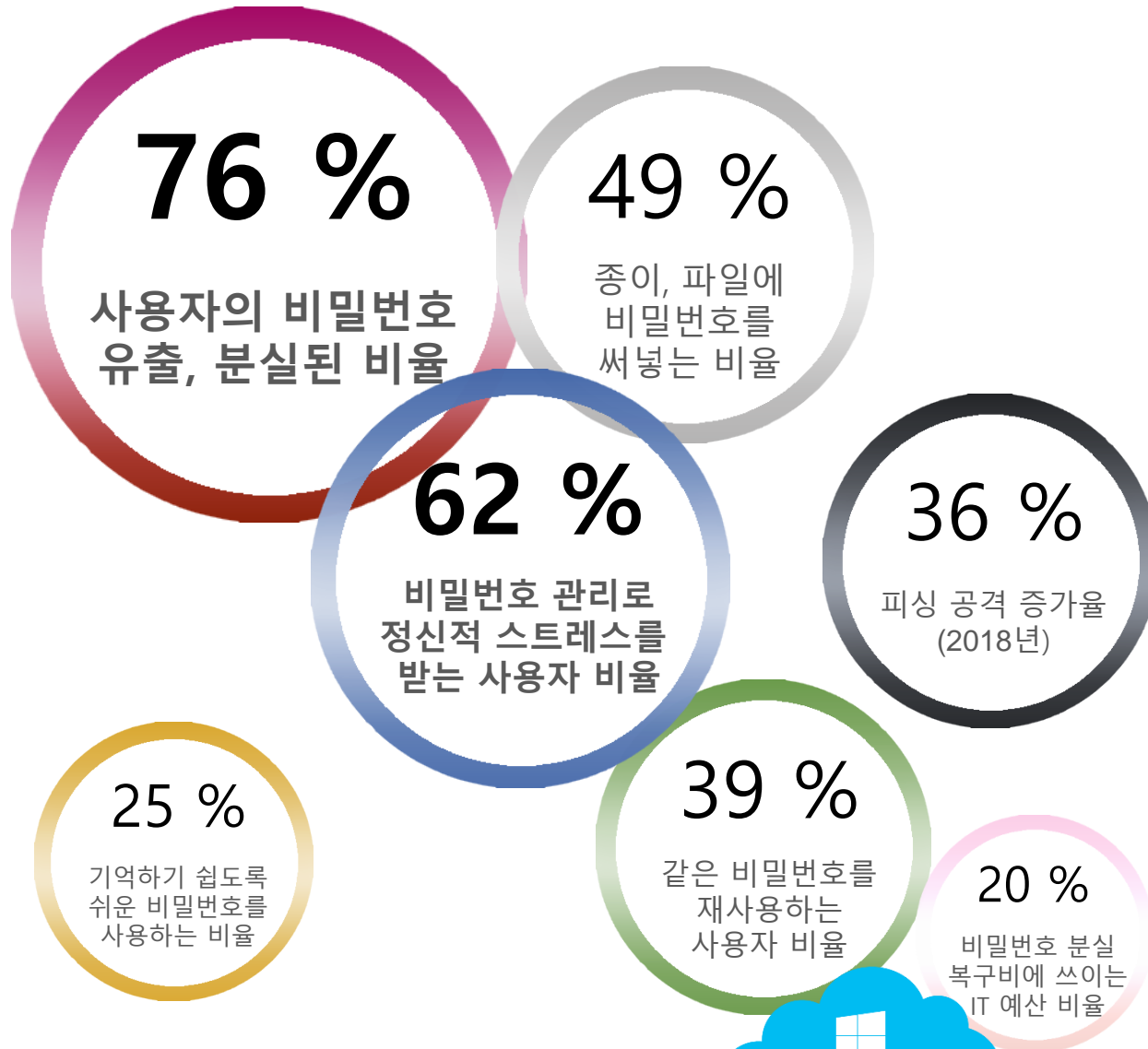
미래에셋대우가 항공기 인수거래를 하던 중 500만달러(약 61억원) 규모의 이메일 해킹(피싱) 피해를 당했다.

이에 과학기술정보통신부는 '코로나19'로 인한 재택·원격근무 시 기업의 해킹 피해를 예방하기 위해 사용자와 보안관리자가 지켜야할 사항을 담은 정보보호 실천 수칙을 권고했다.

## 해커가 노리는 것은?



# 비밀번호의 문제점 및 취약점



**2.3B** 비밀번호 정보 탈취  
(2017 한해 기준)

**279일** 데이터 유출 사건이 발생하는 평균 주기

**\$3.9M** 데이터 유출로 인한 기업의 평균 피해액

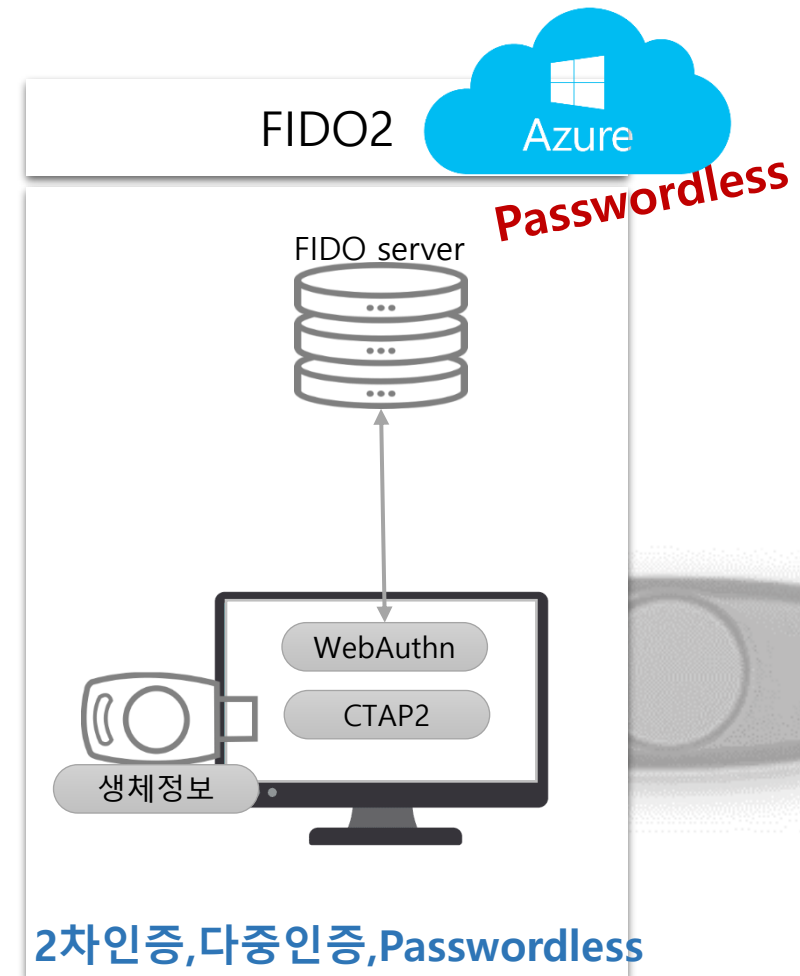
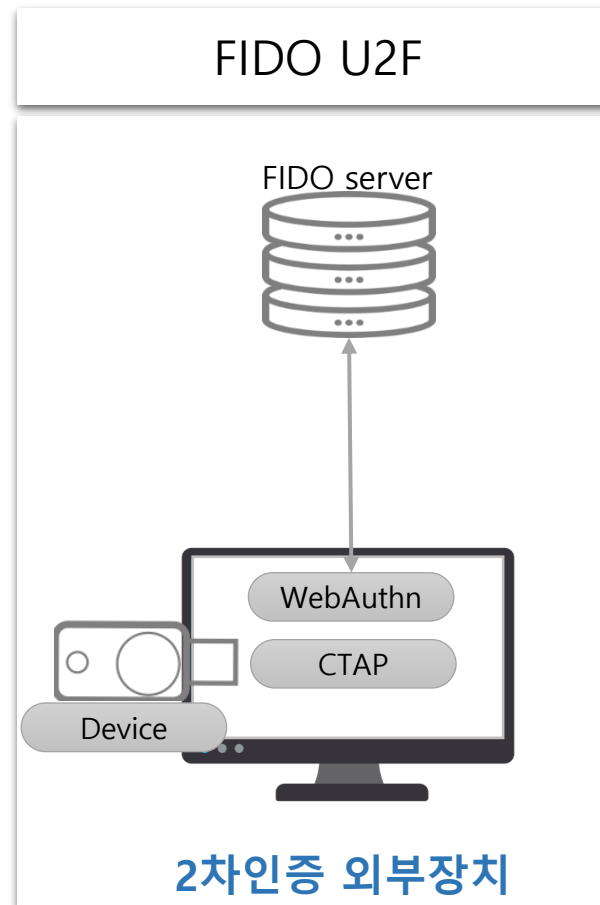
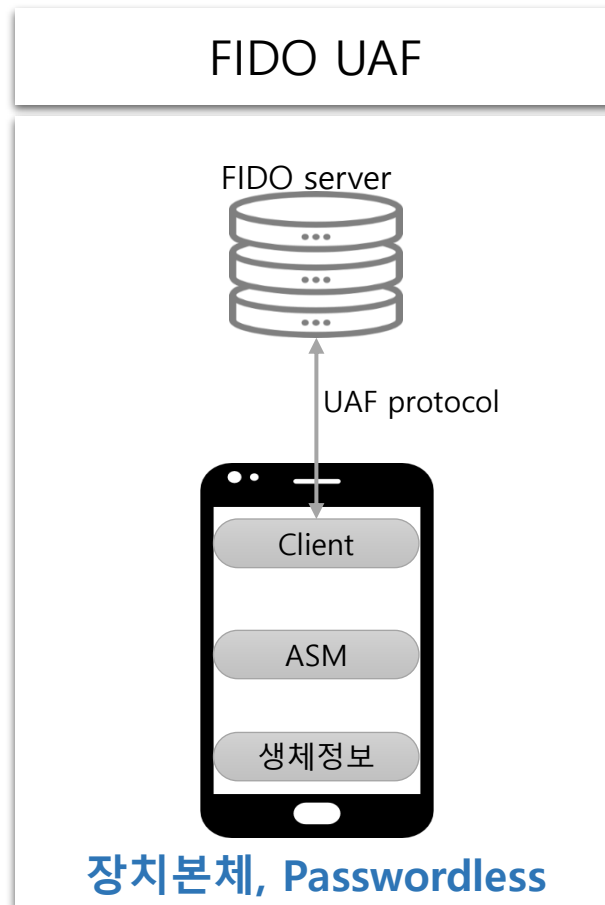
**26K** 데이터 침해시, 탈취되는 평균 record 수량

문제의 해결점은 Passwordless

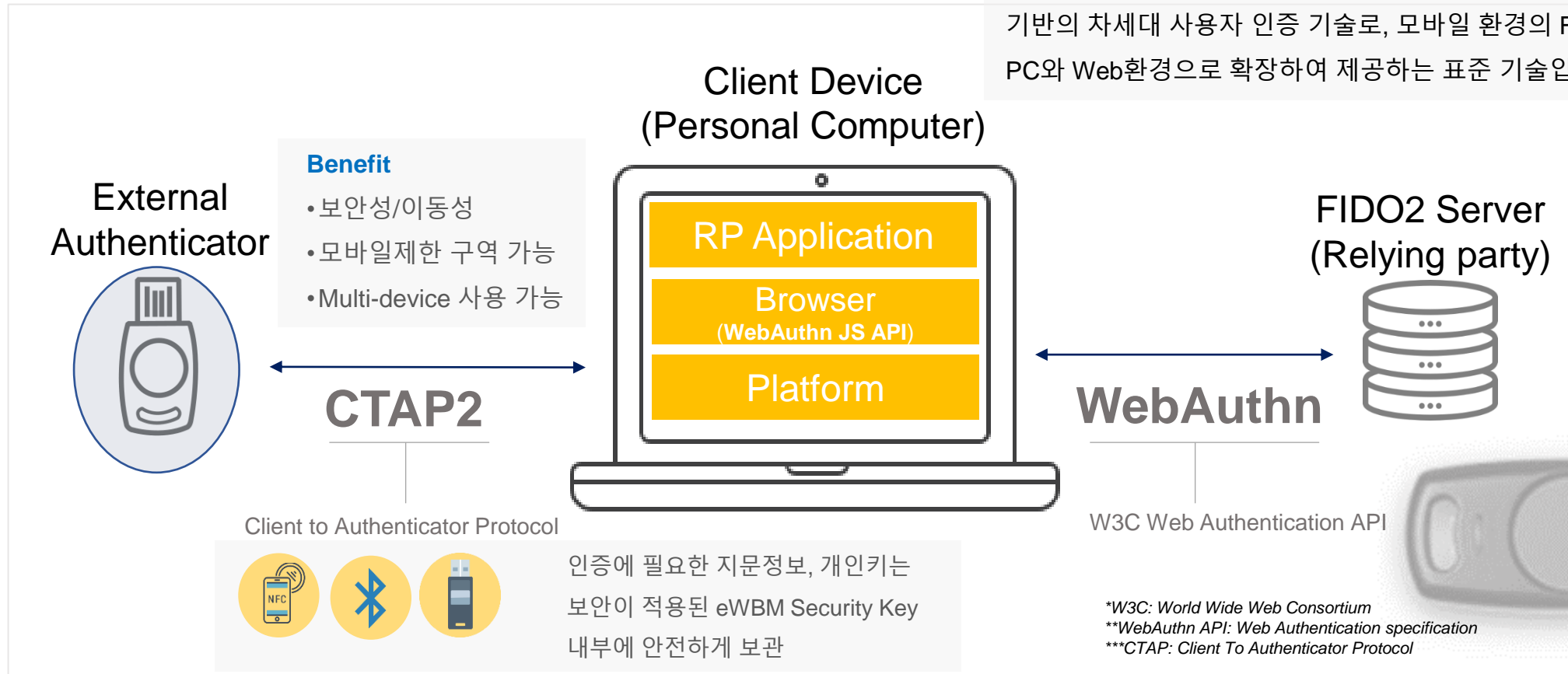




**FIDO**(Fast IDentity Online) **얼라이언스**(Alliance)는 온라인 환경에서 비밀번호를 대체하는 안정성이 있는 인증방식인 FIDO 기술표준을 정하기 위해 2012년 설립된 단체이며, 회원사로 MS, 구글, 삼성전자 등 260여개 회원사가 있음.

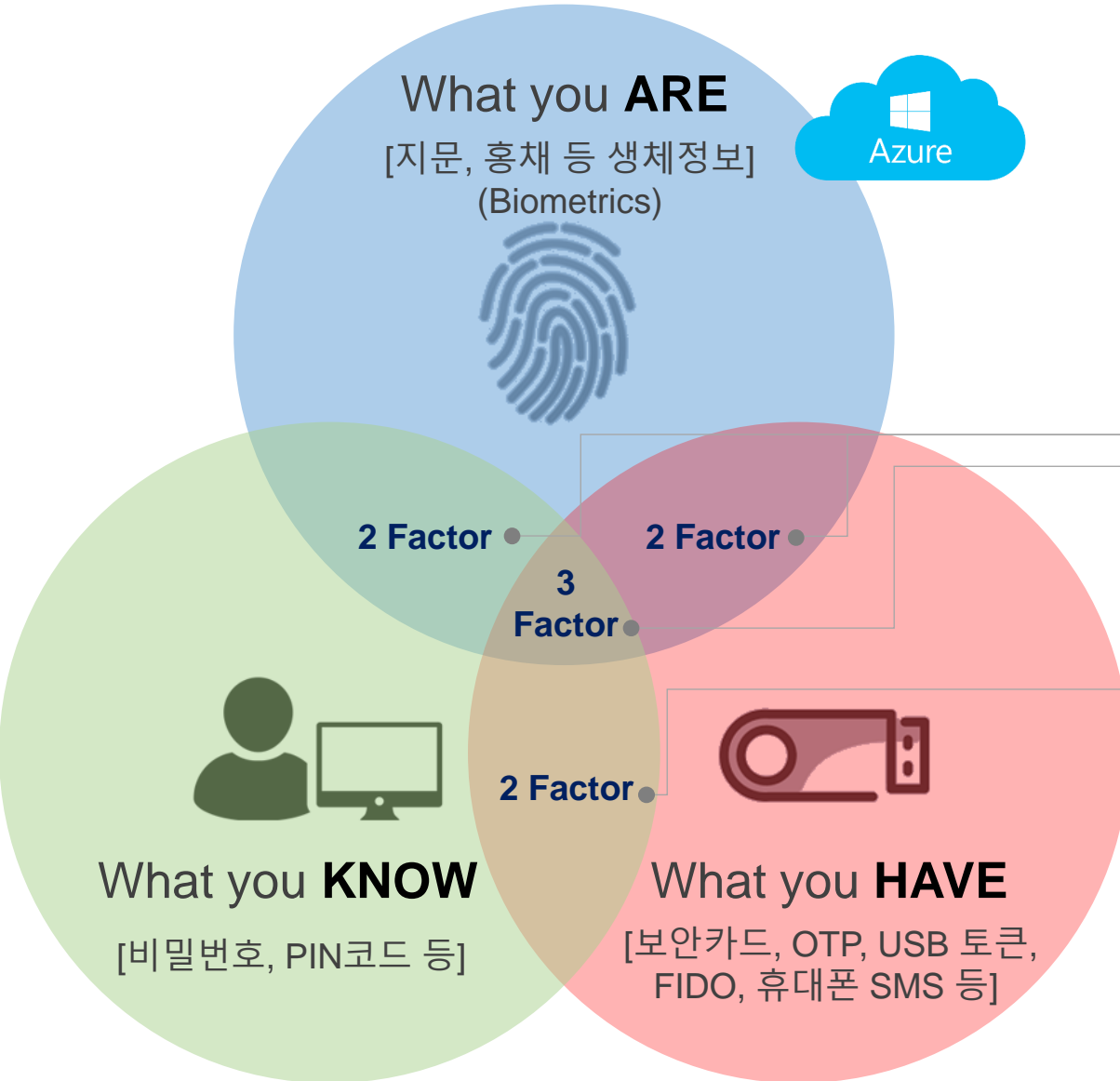


**FIDO**는 온라인 환경에서 지문, 홍채, 안면 인식 등 생체인식 기반의 차세대 사용자 인증 기술로, 모바일 환경의 FIDO 1.0과 PC와 Web환경으로 확장하여 제공하는 표준 기술입니다.



# eWBM FIDO Security Key

## 세계 최초/유일의 FIDO2 Level 2 보안키



- 하드웨어 기반 강력한 인증보안키
- 생체 인식 기술 이용한 추가 보안 수단 (G310/G320)
- 스웨덴의 Precise Biometric(사)의 정품 지문인식 알고리즘
- 휴대성 및 용이성 제고 – No Battery, No program download for use
- USB Type A & Type C
- Supported OS: Windows, macOS, Chrome, Linux



T110 / T120



G310 / G320

강력한 보안



FIDO2 기반의 공개키 및 개인키 암호화를 통해 빠르고 쉬운 로그인 환경의 강력한 보안 기능 제공

배터리 없이



별도의 전원 공급 없이 USB 포트에 꽂아 사용 가능

누구나 쉽고



G320을 USB 포트에 삽입한 후 PC 또는 Mac에서 바로 사용 가능

휴대가 편리한



휴대하기 편리한 초경량 보안키

단 하나의 키

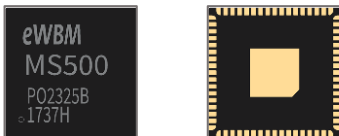


G320을 사용하여 다양한 온라인 서비스에서 지문 등록 및 로그인 가능



# eWBM FIDO Security Key is

## 보안 MCU MS500



- **보안 적용된 부팅**

Firmware가 암호화 및 무결성 검사를 통해 ROM에 저장됨

- **보안이 적용된 저장 공간**

데이터를 Crypto 사용하여 저장장치에 안전하게 저장됨

- 플래시 메모리의 보안 저장 영역에 데이터 저장
- 특정 크기 단위로 데이터 암호화 (e.g. 4KB)

- **High-Speed TRNG (25Mbps): FIPS140-2 Compliant**

- ✓ Security Key의 보안 MCU인 MS500의 보안 저장 영역에 지문 데이터가 암호화되어 저장됨
- ✓ 지문 등록 과정에서 지문 데이터는 PC에 저장되거나 남지 않음
- ✓ 인증 프로세스 중에도 지문 데이터가 외부로 일체 유출되지 않음

## 세계적인 첨단 생체인증 알고리즘 채택



- 지문 인식 알고리즘 기술로 전세계적인 인정을 받은 스웨덴의 프리사이즈 바이오 메트릭스 사의 지문인식 알고리즘을 적용.
- 편리한 지문등록과 최상의 사용 경험을 제공.

**PRECiSE**  
BIOMETRICS



## 연계서비스



# eWBM FIDO Security Key specifications

## T110 / T120



### Product Specifications

FIDO 표준	FIDO2 , U2F
FIDO 보안 인증 등급	Level 1
USB 타입	Type A / Type C
상태 표시	Solid Color LED (White)
터치 방식	정전식
장치 타입	HID device
장치 재질	PC (Polycarbonate)
품질 인증	KC, CE, FCC
사이즈	41.8 x 17.8 x 3.9 mm
무게	2.9 g

### Security Features

Secure Boot
Secure Storage
High-Speed TRNG(25Mbps): FIPS140-2 표준 준수

### Platform · Environment

지원 플랫폼	Windows PC, Mac, iPadOS, Linux, Chromebook, Android etc.
지원 브라우저	Chrome, Edge, Firefox, Safari
Key Manager <sup>3</sup> 지원 OS	Windows, macOS, Linux

## G310 / G320



### Product Specifications

FIDO 표준	FIDO2 , U2F
FIDO 보안 인증 등급	Level 2
USB 타입	Type A / Type C
지문 인식 해상도	160 x 160 pixel
상태 표시	3 Color LED
장치 타입	FIDO2 HID device
지문 알고리즘	Precise™ Biometrics
사이즈	41.9 x 17.8 x 4.4 mm
무게	3.1 g

### Cryptography Algorithm List

Confidentiality	AES-256
Hashing	SHA-256
Data Authentication	HMAC
Key Protection	GCM Mode, with fixed length 96 bit IVs
Signature	ECDSA, ECDH

### FIDO2 Level 2 Security Features

Secure Boot
Secure Storage
High-Speed TRNG(25Mbps): FIPS140-2 표준 준수

Designed and manufactured in Korea

Copyright © eWBM Co., Ltd. All rights reserved.

# Microsoft's password replacement offerings

Standards-based private key authentication that is convenient and more secure than a password



Windows Hello for Business  
(FIDO2)



Microsoft Authenticator



FIDO2 security keys



# Passwordless with FIDO2 security keys

Microsoft uses open standards that work with innovative offerings from partners

USB/NFC Key



USB Biometric Key

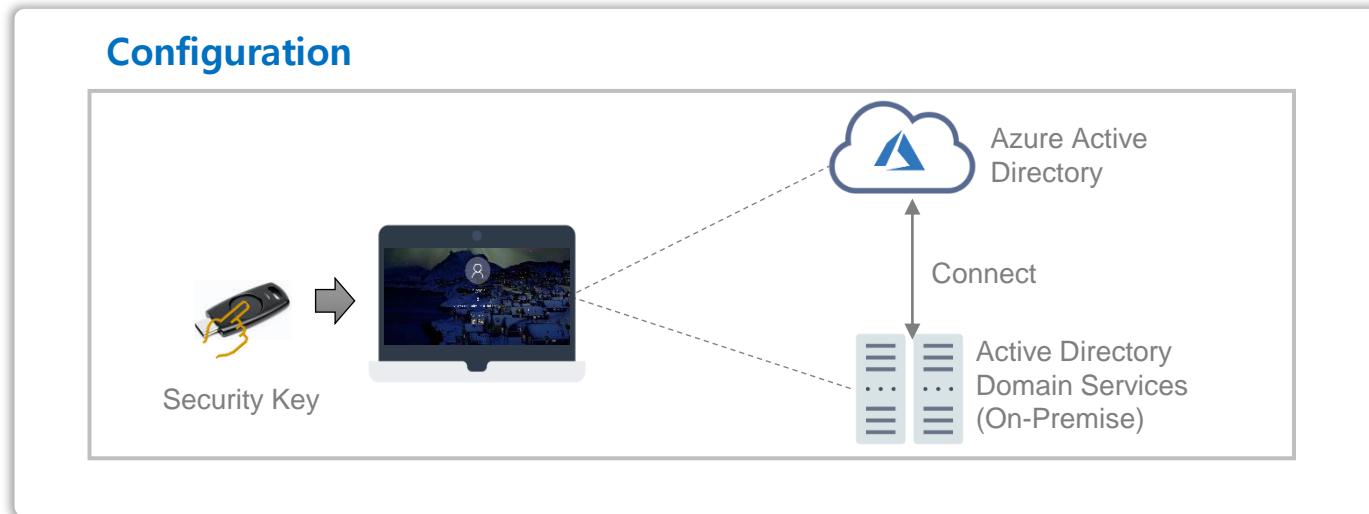


NFC Badges & Wearables






## "Microsoft Azure MFA 기능지원 "

- Azure MFA 로 새롭게 출시되는 Security Key 기능 지원
- Azure MFA 기능 지원
  - 동일한 Cloud(Office365) 환경에서 Security key를 이용한 Windows Logon 가능
- Hybrid Azure MFA 기능 지원
  - 동일한 Domain 환경에서 Security key를 이용한 Windows Logon 가능





- 등록 (Registration) 
- 인증 (Authentication)
  - Windows login with Azure AD 
  - Microsoft.com login with passwordless 





# eWBM

---

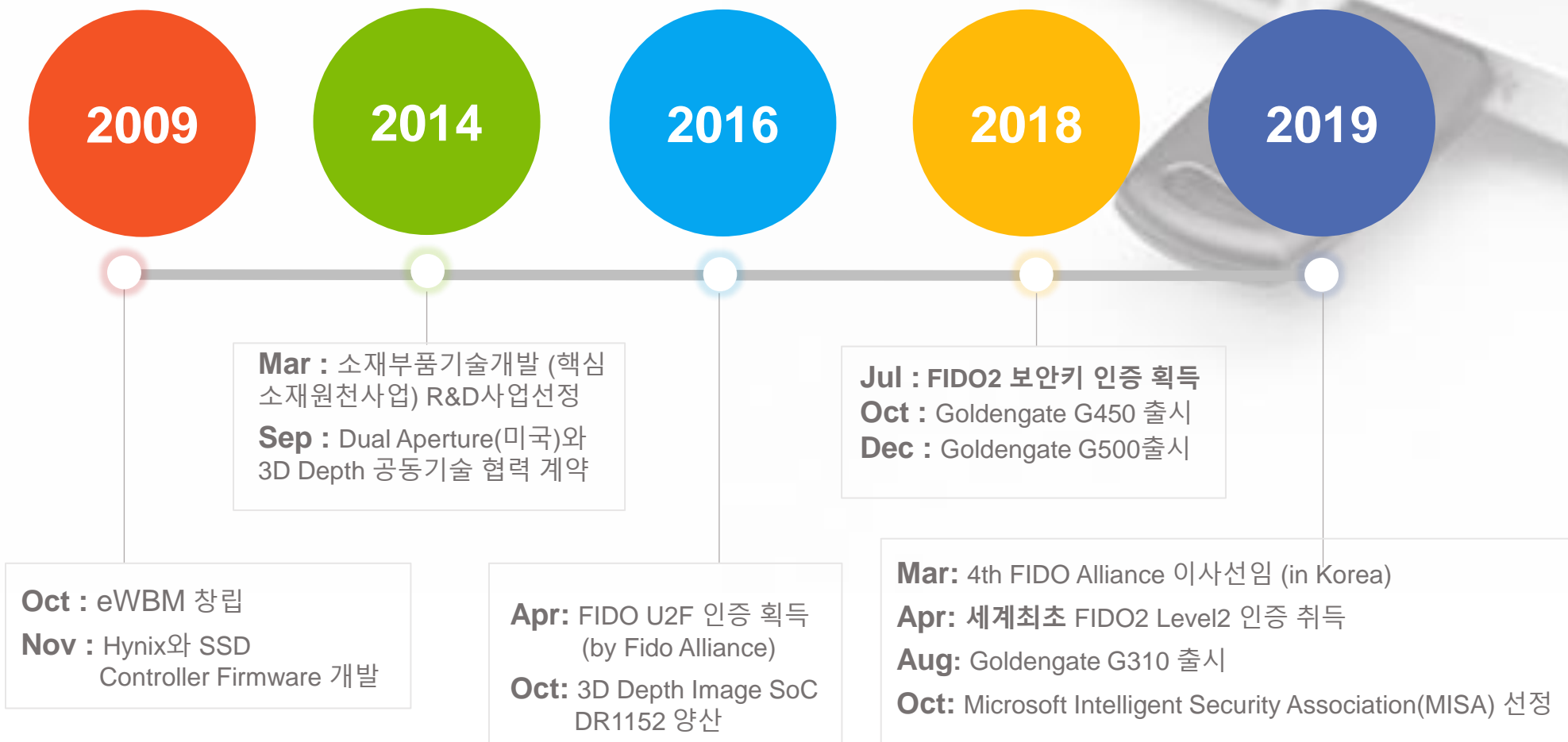
Company Profile : [www.ewbm.com](http://www.ewbm.com)

**Founded on** 2009년 10월 15일

**CEO:** Stephen Oh, Ph.D.

**R&D Center:** 서울특별시 강남구 테헤란로20길 9, 14층 06236 (역삼동 동궁빌딩)

**US Office:** 2100 Alamo Rd Suite T, Richardson, TX



# eWBM / TRUSTKEY is **fido**™ Board Level Member ALLIANCE

- FIDO Alliance 이사회 멤버는 글로벌 정책 및 시장 개발 활동에 참여하여 FIDO Alliance의 전세계 시장에서 FIDO 인증 기술을 확장하려는 전략에 대한 리더십과 지침을 제공합니다.
- 이사회 멤버는 FIDO Alliance의 모든 실무 그룹과 총회, 본회의에서 보안인증 관련 정책 및 솔루션에 대한 의사결정에 참여하는 의결권을 보유할 수 있게 됩니다.

**fido**™  
ALLIANCE | simpler  
stronger  
authentication

**An Industry  
Movement to  
Provide  
Passwordless  
Solutions**



[FIDO 이사회 멤버]



is now



[Securing the World for Everyone, Everywhere]

## Microsoft Intelligent Security Association

MISA(Microsoft 지능형 보안 연합)는 점점 증가하는 사이버 위협에 대비하기 위하여, 솔루션을 통합한 독립 소프트웨어 공급업체의 에코시스템입니다.

[Learn more](#)



eWBM은 급격하게 늘어나는 정교한 사이버 위협에 대응하기 위하여 혁신적이고 높은 수준의 사이버 보안 기술을 제공하는 기업으로 구성된 MISA\*멤버에 합류하여 Microsoft와 긴밀하게 협력하고 있습니다.

MISA에 포함되어 있는 제품을 이용하는 기업과 기관이 eWBM의 Goldengate Security Key를 아이덴티티 및 액세스 관리 분야에 쉽게 적용할 수 있게 되었다는 것을 의미합니다.



# 4. FIDO Certification (인증서)



- FIDO 2 Authenticator : G310



- FIDO 2 Authenticator : G320



- FIDO2® Server Certification



- FIDO® U2F Certification

## FIDO Security Level 1

### 보안 요구 사항

1. 인증기 정의 및 파생된 인증기 요구 사항 (10 articles)
2. 키 관리 및 인증기 보안 매개 변수 (23 articles)
3. 인증기의 사용자 유무 및 사용자 확인테스트 (8 articles)
4. 개인 정보 보안 (5 articles)
5. 물리적 보안 (0 article)
6. 증명 (2 articles)
7. 운영 환경 (0 article)
8. 자체 검사 및 펌웨어 업데이트 (1 article)
9. 제조 및 개발 (3 articles)

### 암호 알고리즘

제한 없음

### 작동 환경

제한 없음

### Level 2 인증은

원치 않는 응용 프로그램 다운로드,

악성 웹 콘텐츠 등으로 오염된

운영체제의 접근으로부터,

생체정보 및 사이트 액세스 자격 증명

등의 결정적 정보를 보호하기 위해

TEE 또는 SE와 같은 제한된

운영 환경을 구현해야 하는 등의

한층 더 강화된 보안조건 입니다.

## FIDO Security Level 2

### 보안 요구 사항

1. 인증기 정의 및 파생된 인증기 요구 사항 (10 articles)
2. 키 관리 및 인증기 보안 매개 변수 (+3 articles)
3. 인증기의 사용자 유무 및 사용자 확인테스트 (8 articles)
4. 개인정보 보안 (5 articles)
5. 물리적 보안 (+3 articles)
6. 증명 (+3 articles)
7. 운영 환경 (+6 articles)
8. 자체 검사 및 펌웨어 업데이트 (+2 articles)
9. 제조 및 개발 (+3 articles)

### 암호 알고리즘

FIDO Authenticator Allowed Cryptography List Compliant

- 112 bit 이상의 암호 강도 (당사 Security Key 암호 수준: 128 bit)
- 기밀성, 해싱, 데이터 인증, 키 보호, TRNG (True Random Number Generator), 키 생성, 서명 알고리즘.

### 작동 환경

인증기가 허용된 제한된 운영 환경 (AROE).

- ARM Trust Zone, Intel VT, TPM, Secure Element (SE)와 같은 제한된 운영 환경 필요함

Source : FIDO Authenticator Security Requirements

FIDO2 Level 2는 Fido Alliance에 존재하는 가장 높은 보안 등급입니다.

eWBM의 Goldengate Security Key는 세계 최초의(현재까지 유일한) FIDO2 Level 2 인증 디바이스 입니다.

Model Series	T110	T120	G310	G320	G450	G500
						
FIDO 표준	FIDO2, U2F	FIDO2, U2F	FIDO2, U2F	FIDO2, U2F	FIDO2, U2F	FIDO2, U2F
FIDO 보안 인증 등급	Level 1	Level 1	Level 2	Level 2	Level 2	Level 2
지문 인식 알고리즘	-	-	Precise™ Biometrics	Precise™ Biometrics	Precise™ Biometrics	Precise™ Biometrics
USB 타입	Type A	Type C	Type A	Type C	Type A	Type A
지문 인식 해상도	-	-	160x160 pixels	160x160 pixels	160x160 pixels	160x160 pixels
보안 MCU	MS500	MS500	MS500	MS500	MS500	MS500
하드웨어 알고리즘	AES, HMAC, SHA, ECDSA, ECDH					
보안 및 기타 인증	FIPS <sup>1)</sup> 140-2, 140-3 Compliant, FCC <sup>2)</sup> , CE <sup>3)</sup> , KC <sup>4)</sup> , RoHS <sup>5)</sup>					
무게	2.9g	2.9g	3.1g	3.1g	6.6g	31.2g
소재	PC	PC	PC	PC	플라스틱	Zn-alloy
슬리브 / 캡	-	-	-	-	O	O
출시 년도	20.Q1	20.Q1	19.08	20.Q1	18.10	18.12

FIPS<sup>1)</sup>: 연방 정보처리 규격 (Federal Information Processing Standards)

FCC<sup>2)</sup>: 미국연방통신위원회 (Federal Communications Commission)

CE<sup>3)</sup>: 유럽경제지역(EEA) 내에서 판매되는 제품의 건강, 안전 및 환경 보호 표준 준수를 나타내는 인증

KC<sup>4)</sup>: 대한민국 국가통합인증

RoHS<sup>5)</sup>: 유해물질 제한지침(Restriction of the use of Hazardous Substances)

A blurred background image showing a silver laptop and a black USB drive plugged into a port on the side of the laptop.

# 감사합니다.

---

[www.ewbm.com](http://www.ewbm.com)

# FIDO series

