DualAuth

OWASP Seoul
IoT 서비스에서 온/오프라인 사용자 보안 인증 동향

듀얼오스 우종현 대표

DualAuth

01

소개

02

IoT 보안 사고와 주요 요인

03

온/오프라인 IoT 서비스 인증 동향

04

요약

01 소개

ITU-T SG17 Security Q10 Identity 분과 위원 X.oobsa 신규 기고서 제안

TTA PG 502 개인정보보호/ID관리, 블록체인보안 프로젝트 분과 위원

TTA 인증 비컨 기반 전자출입명부 표준 기술 개발

모바일 운전면허 확인 서비스 기술기준 안 과제 책임자

블록체인 기반 DID 신원인증 기술 개발 과제 책임자

청와대, 우리은행, 한국산업기술진흥원 등 국내 주요기관에 인증기술 공급

상호인증 기술 개발로 대한민국 인터넷 대상 수상

DualAuth

01

소개

02

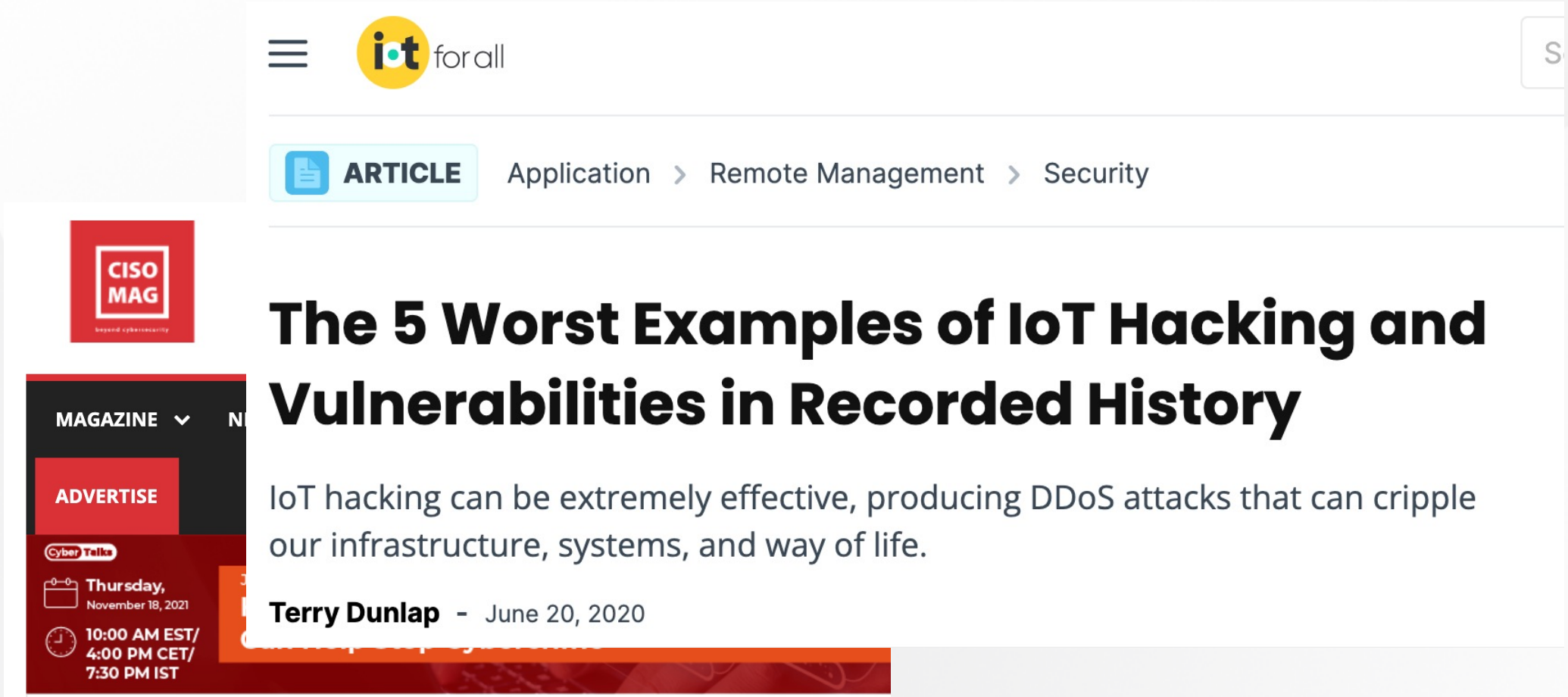
IoT 보안 사고와 인증 기술 유형

03

IoT 서비스 인증 기술 요건 및 표준화 동향

04

요약



iot for all

ARTICLE Application > Remote Management > Security

The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History

IoT hacking can be extremely effective, producing DDoS attacks that can cripple our infrastructure, systems, and way of life.

Terry Dunlap - June 20, 2020

CISO MAG

MAGAZINE

ADVERTISE

Cyber Talks

Thursday, November 18, 2021

10:00 AM EST/ 4:00 PM CET/ 7:30 PM IST

Home > Features > 10 IoT Security Incidents That Make You Feel Less Secure

FEATURES

10 IoT Security Incidents That Make You Feel Less Secure

By **CISOMAG** - January 10, 2020

Stolen credentials

In 96% of Rapid7's findings, a stolen credential was the cause of an incident. The top four industries affected by stolen credentials were:

Credentials = ID + PW (Authentication Method)

계정을 어떠한 인증수단으로 보호해야 할까?

인증과 인증서의 차이

인증과 인증서의 차이

정보 처리 단말기에서, 개인 식별 정보를 확인하는 절차 등을 따라 사용자 본인이 맞는지를 확인하는 일.

문서나 행위가 정당한 절차로 이루어졌음을 인정하여 증명하는 증서.

Authentication Vs. Certificate

support@DualAuth.com

In-Band Authentication

VS

Out-out band Authentication


1 - Username/password
& OTP code
2 - Bind Attempt
3 - Access Accept/Reject
OpenOTP


CRL(Certificate Revocation List)
CA
VA
RA
인증서
인증서
요청서
인증서
전자서명값

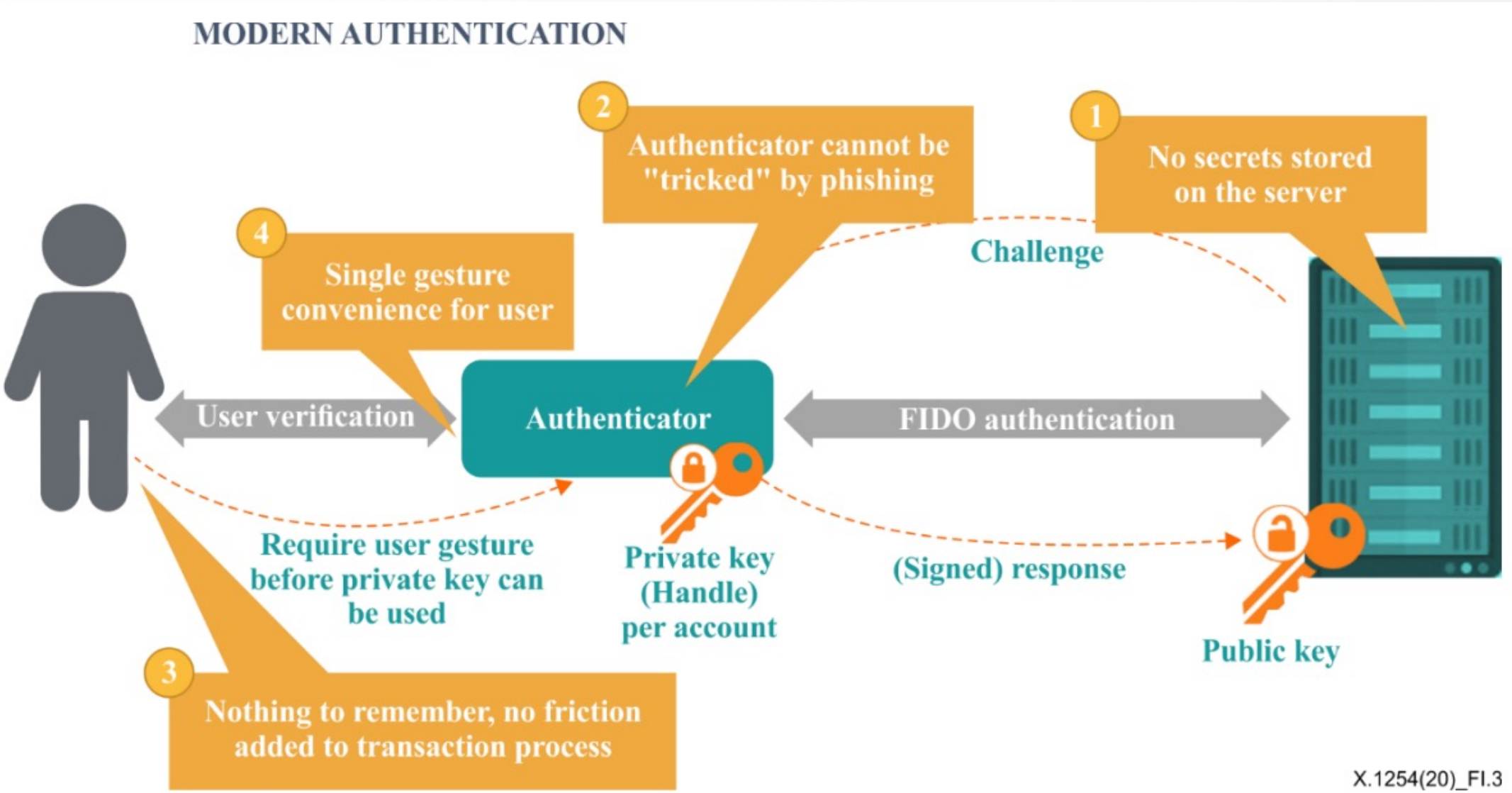
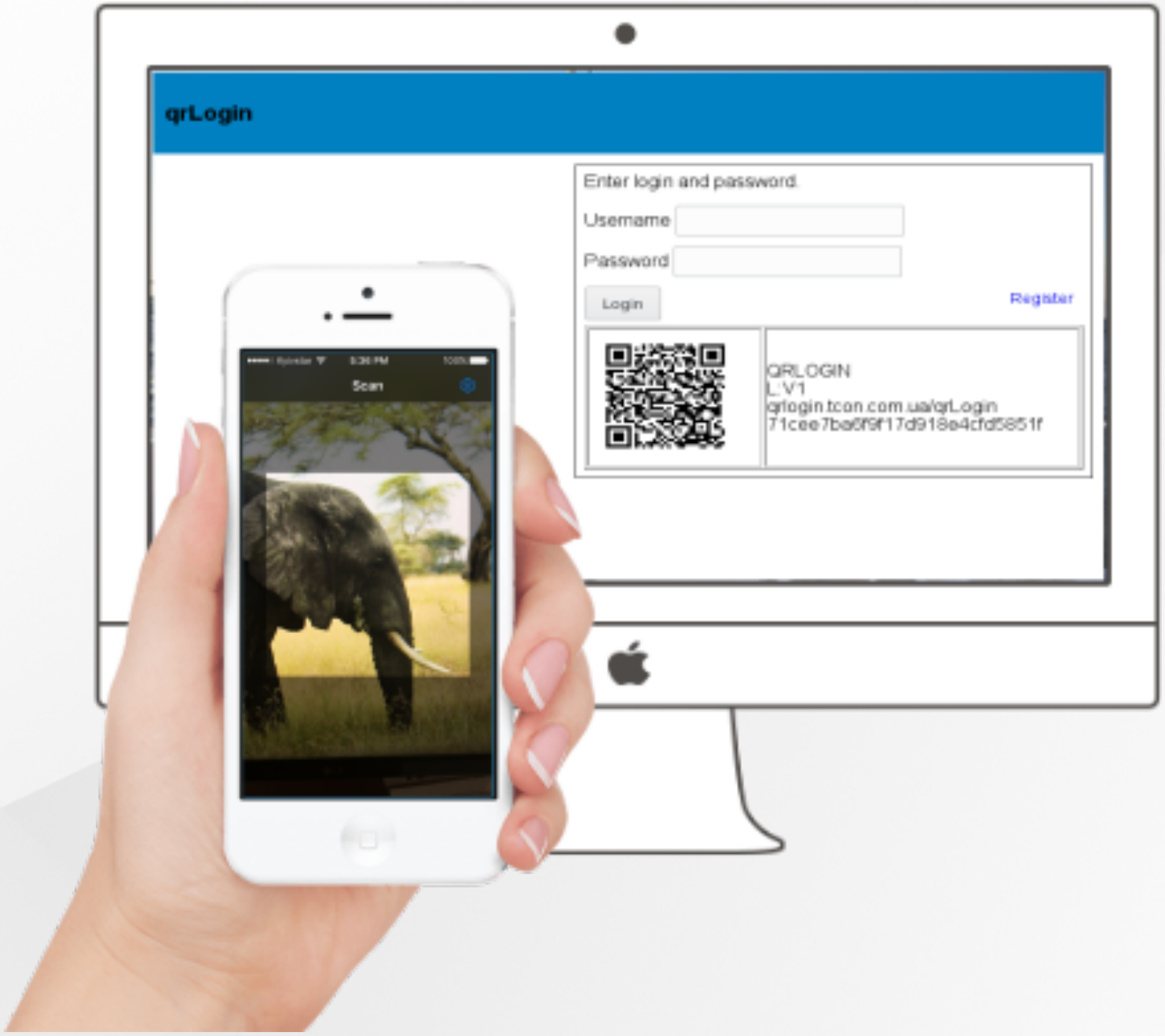
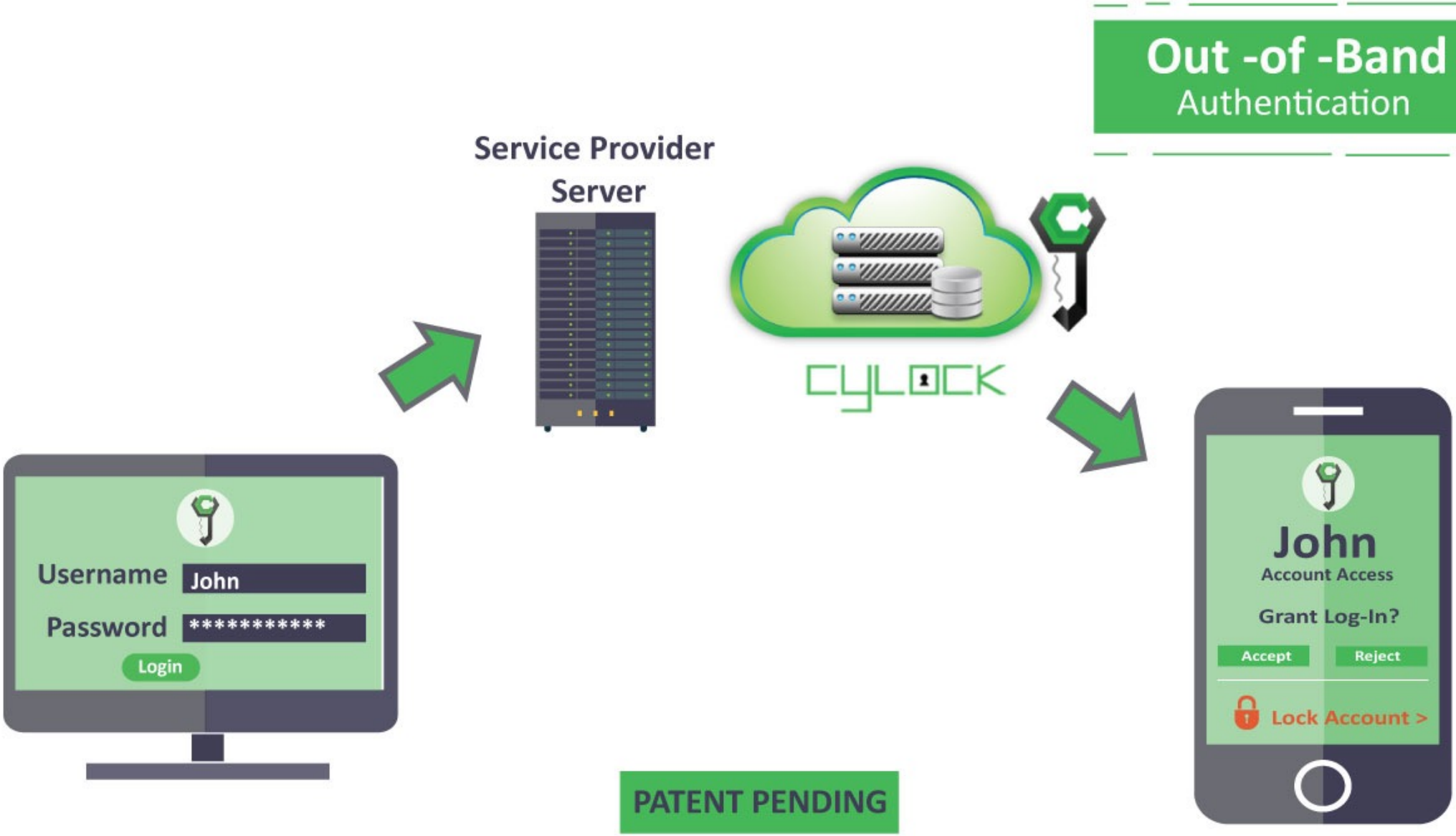
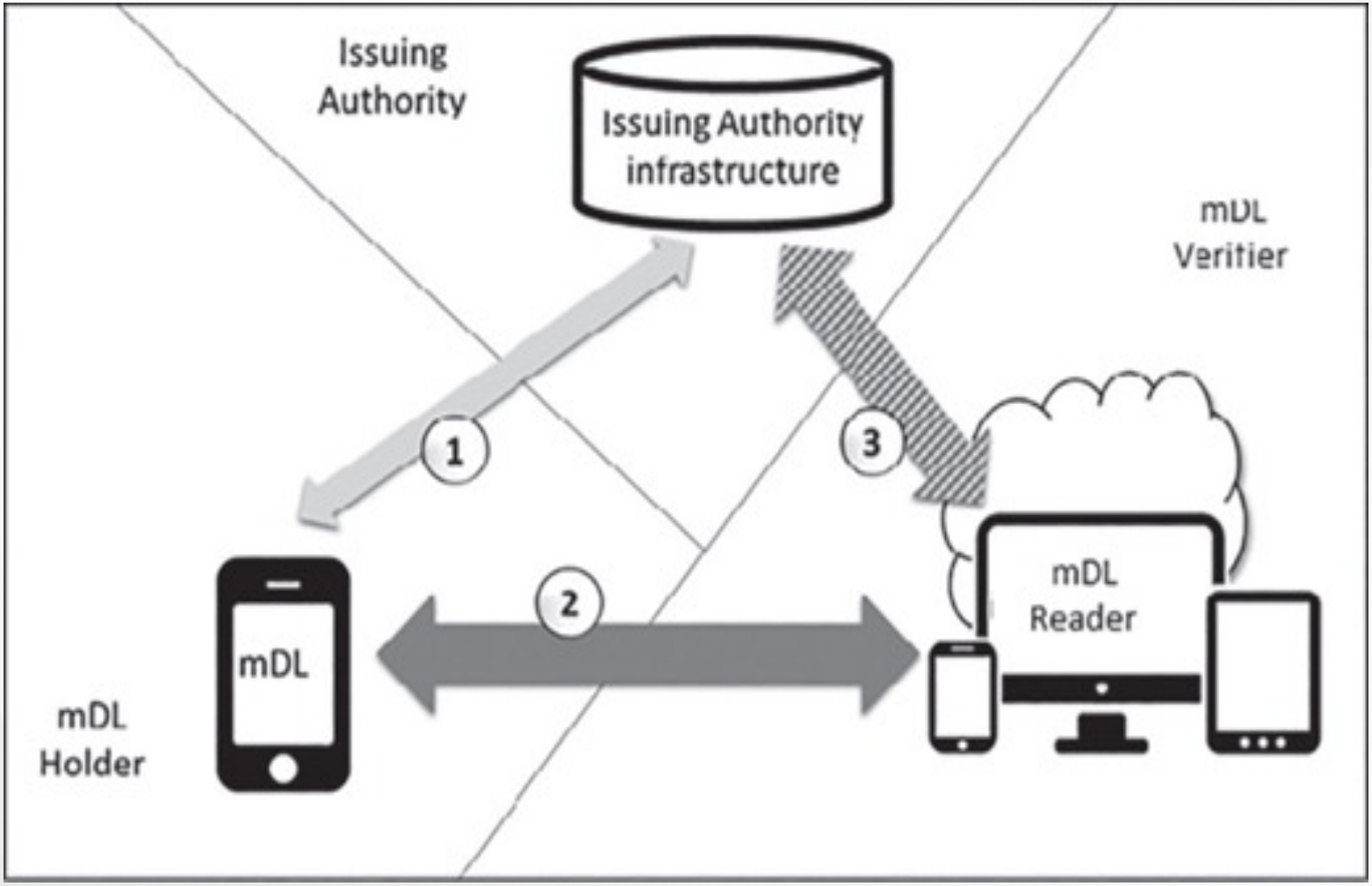
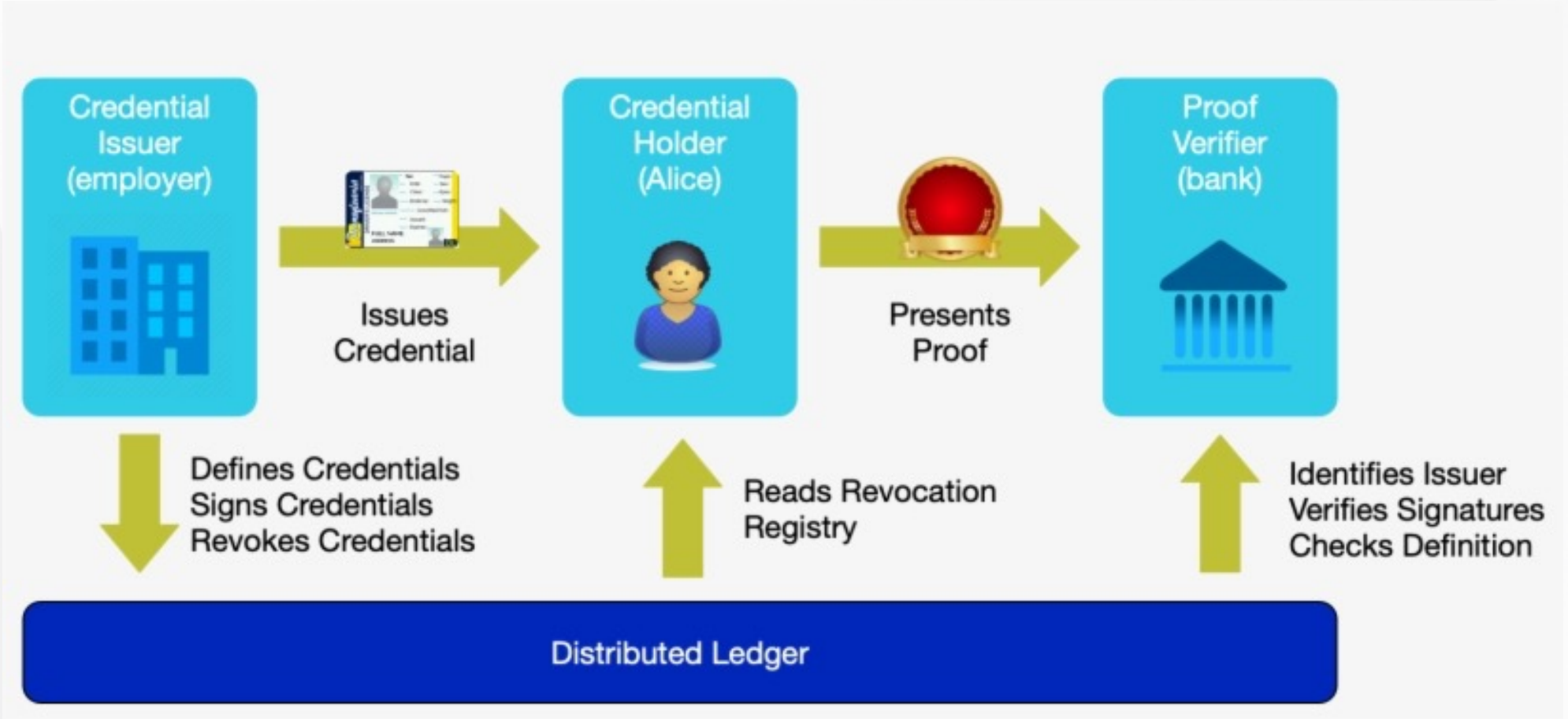


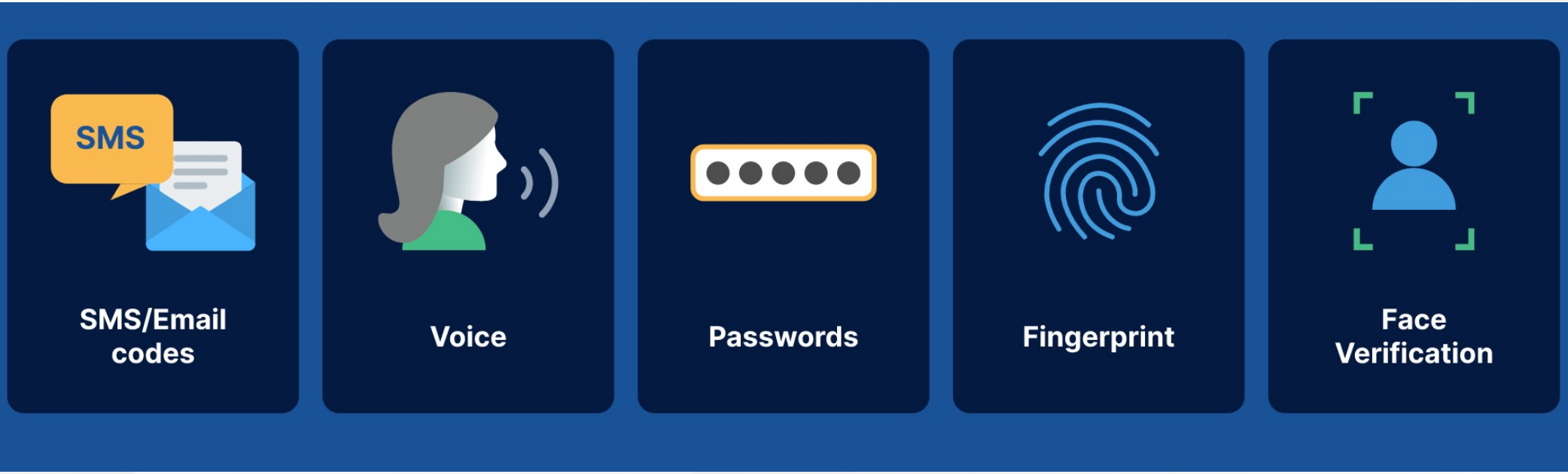
Figure I.3 – New authentication with [b-ITU-T X.1278]

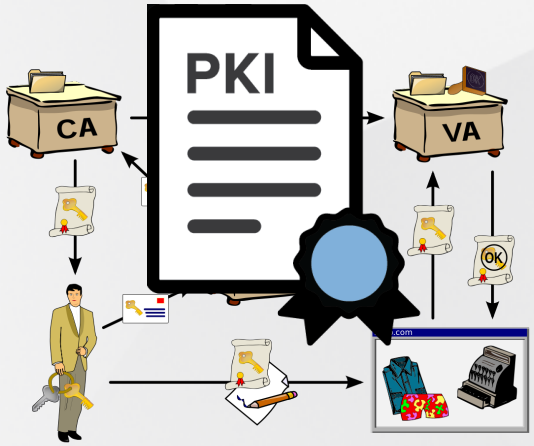

qrLogin
Enter login and password
Username
Password
Login
Register
QRLOGIN
L:V1
qrlogin.tcon.com.ua/qrLogin
71cee7ba6f9f17d918e4cfd5851f
Scan

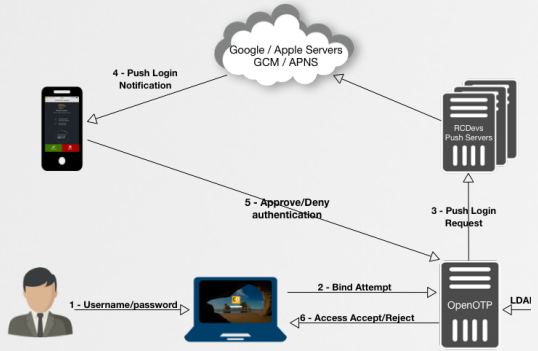

Out -of -Band
Authentication
Service Provider
Server
CyLOCK
Username
John
Password
****
Login
John
Account Access
Grant Log-In?
Accept
Reject
Lock Account >
PATENT PENDING

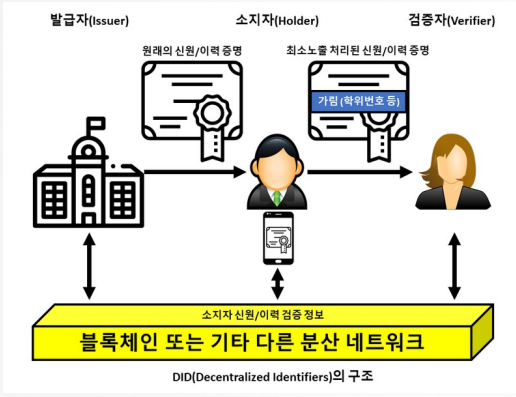

Issuing
Authority
Issuing Authority
infrastructure
mDL
Verifier
1
3
2
mDL
mDL
Reader
mDL
Holder


Credential Issuer (employer)
Issues Credential
Credential Holder (Alice)
Presents Proof
Proof Verifier (bank)
Defines Credentials
Signs Credentials
Revokes Credentials
Reads Revocation Registry
Identifies Issuer
Verifies Signatures
Checks Definition
Distributed Ledger









DID(Decentralized Identifiers)의 구조

Authentication Assurance Level

Table 5-2 Authenticator Assurance Levels

Authenticator Assurance Level
AAL1: AAL1 provides some assurance that the claimant controls an authenticator registered to the subscriber. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator(s) through a secure authentication protocol.
AAL2: AAL2 provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through a secure authentication protocol. Approved cryptographic techniques are required at AAL2 and above.
AAL3: AAL3 provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a “hard” cryptographic authenticator that provides verifier impersonation resistance.

https://pages.nist.gov/800-63-3/

DualAuth

01

소개

02

IoT 보안 사고와 인증 기술 유형

03

IoT 서비스 인증 기술 요건 및 표준화 동향

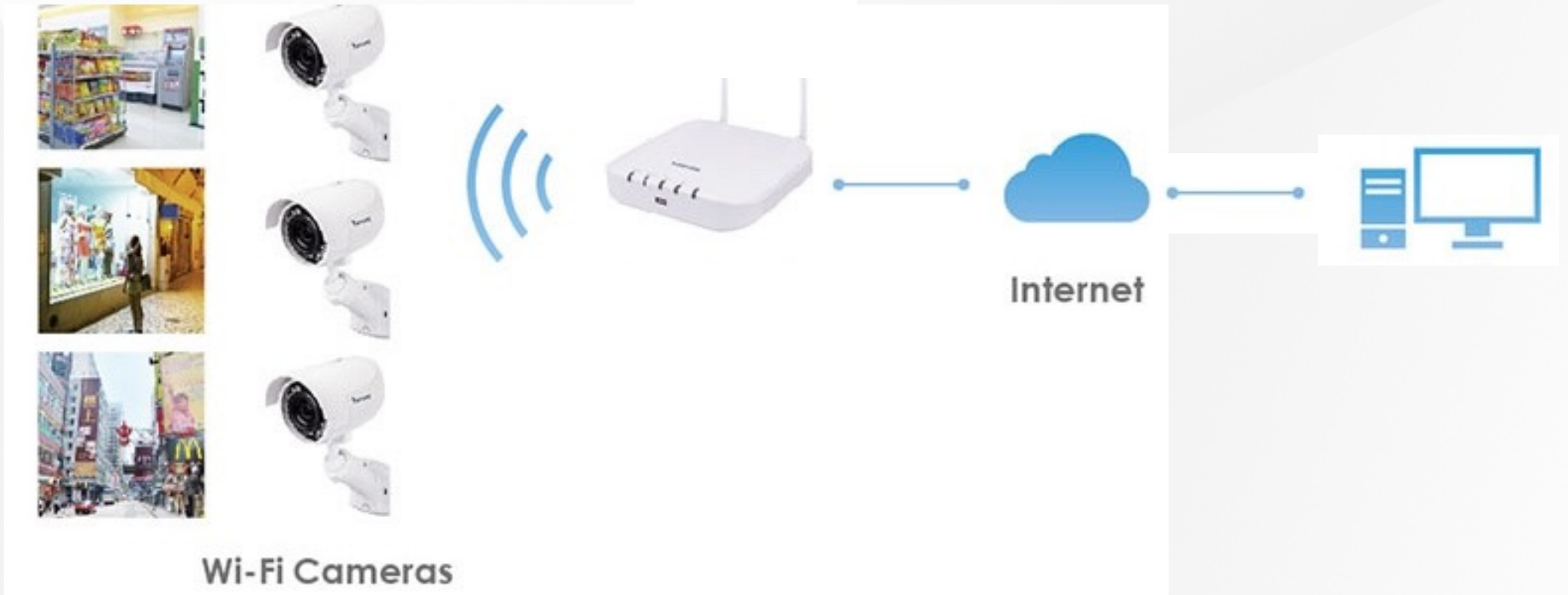
04

요약

IoT 서비스에서 인증기술은 무엇을 고려해야 하나?


Online to Offline

Online IoT Service


Internet
Wi-Fi Cameras


http:\\ Your.Bank
Password?

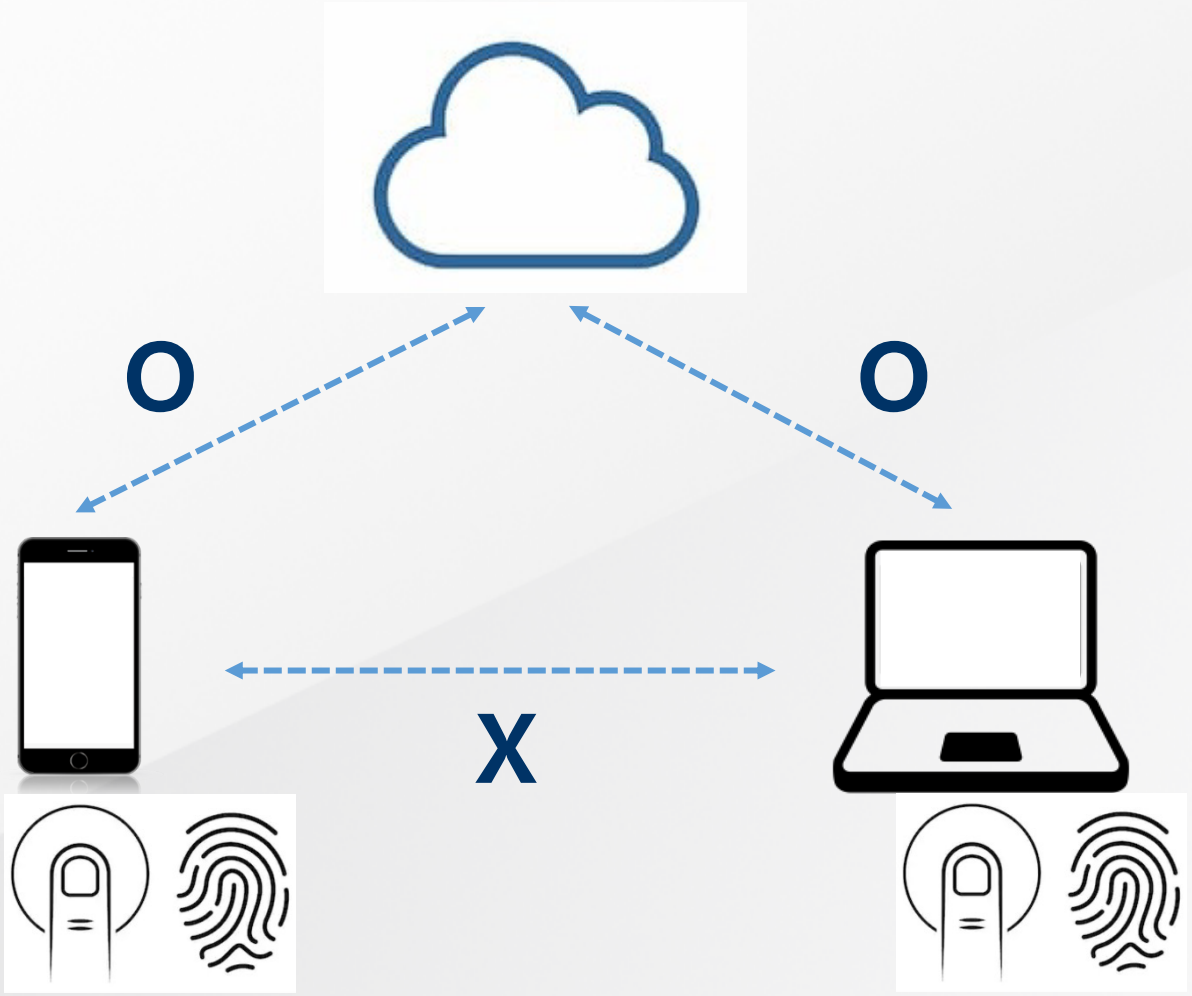
‘파밍’ 확산…해커에 넘어간 공인인증서

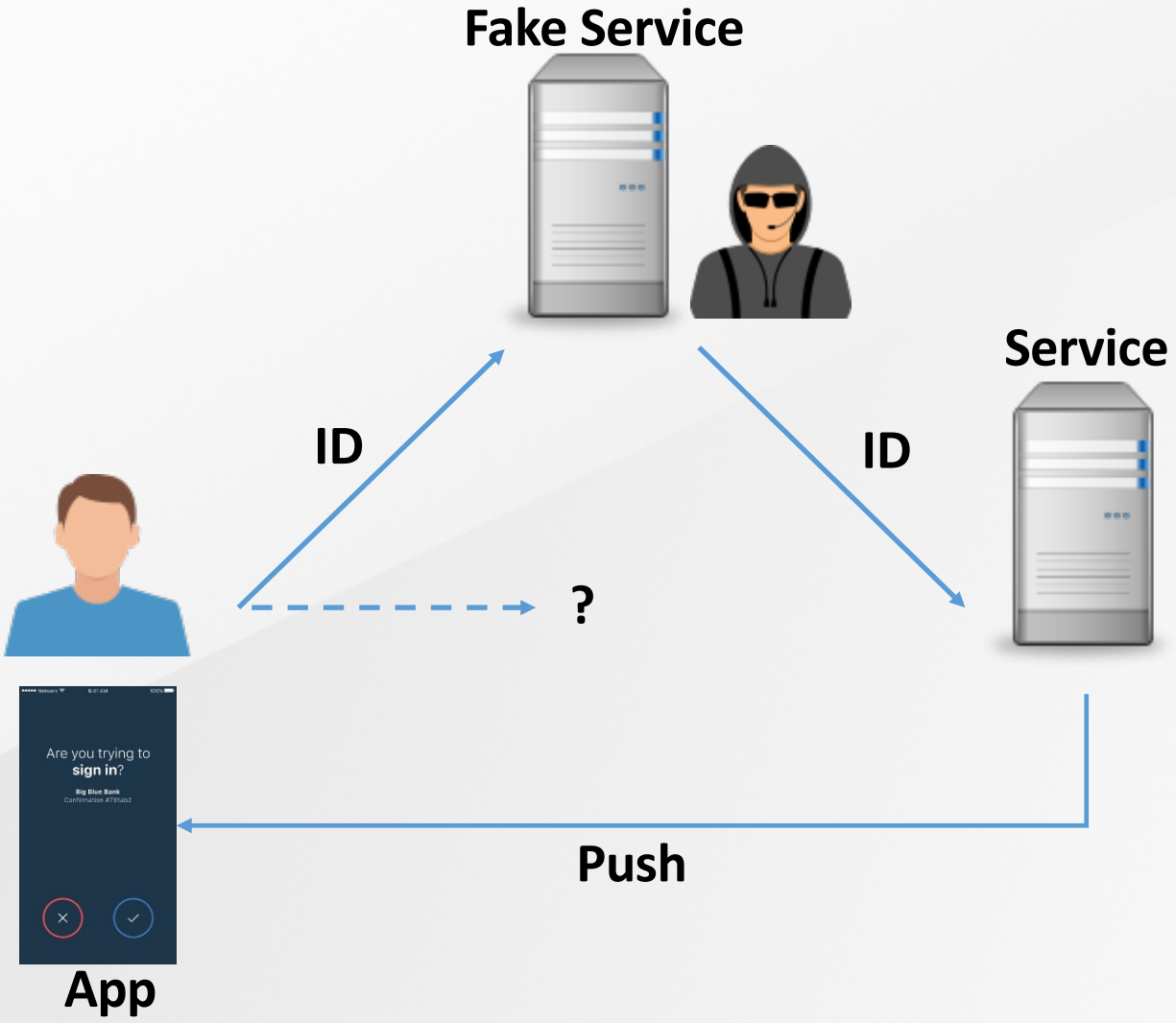
입력 2013.02.12 (07:11) | 수정 2013.02.12 (08:21) 뉴스광장

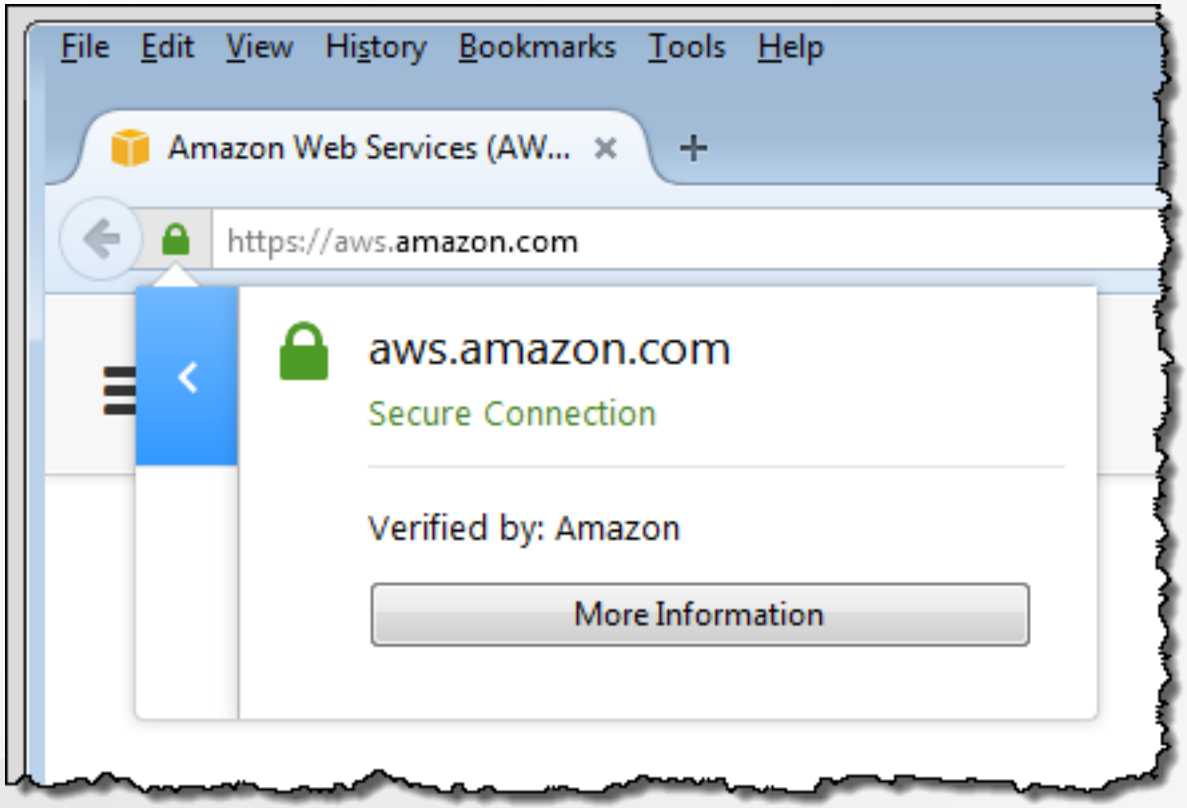
역시 생체인증인가?

여러 단말기에서

온라인 IoT 서비스에 접속하는 상황


O
O
X


Fake Service
Service
ID
ID
?
Are you trying to
sign in?
Push
App


File Edit View History Bookmarks Tools Help
Amazon Web Services (AW...
https://aws.amazon.com
aws.amazon.com
Secure Connection
Verified by: Amazon
More Information

서비스와 사용자를 동시에 인증하는 기술

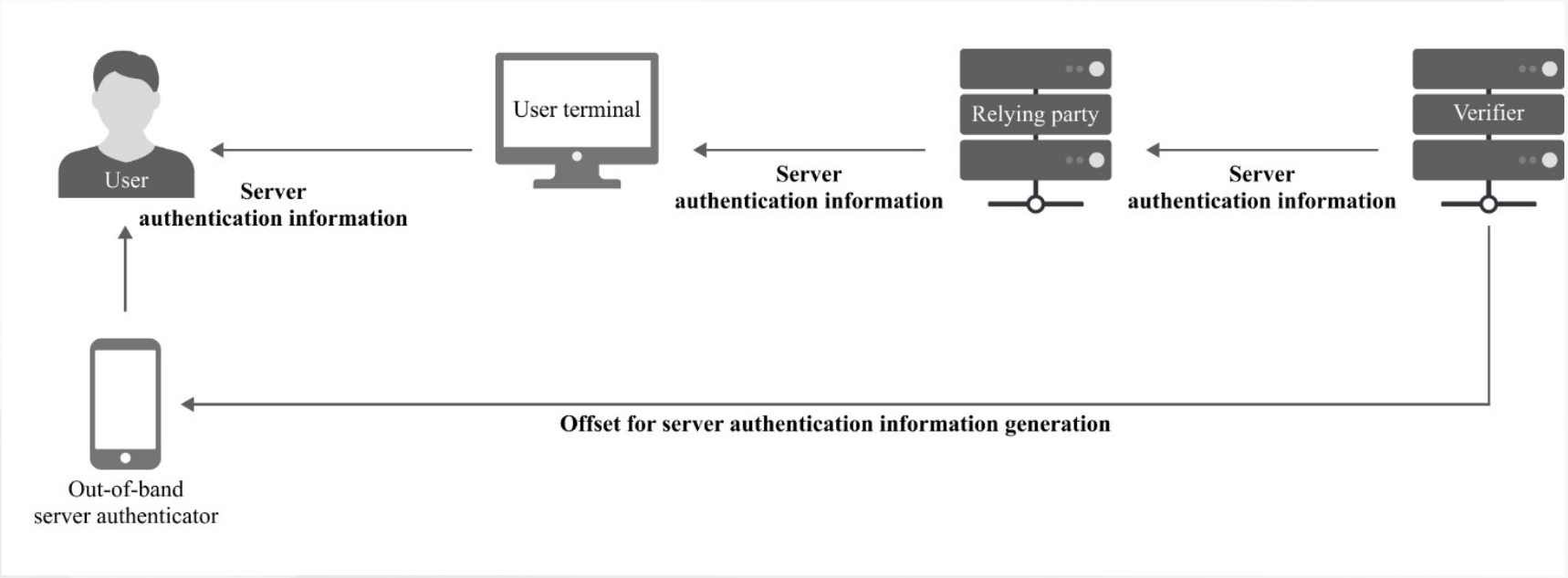
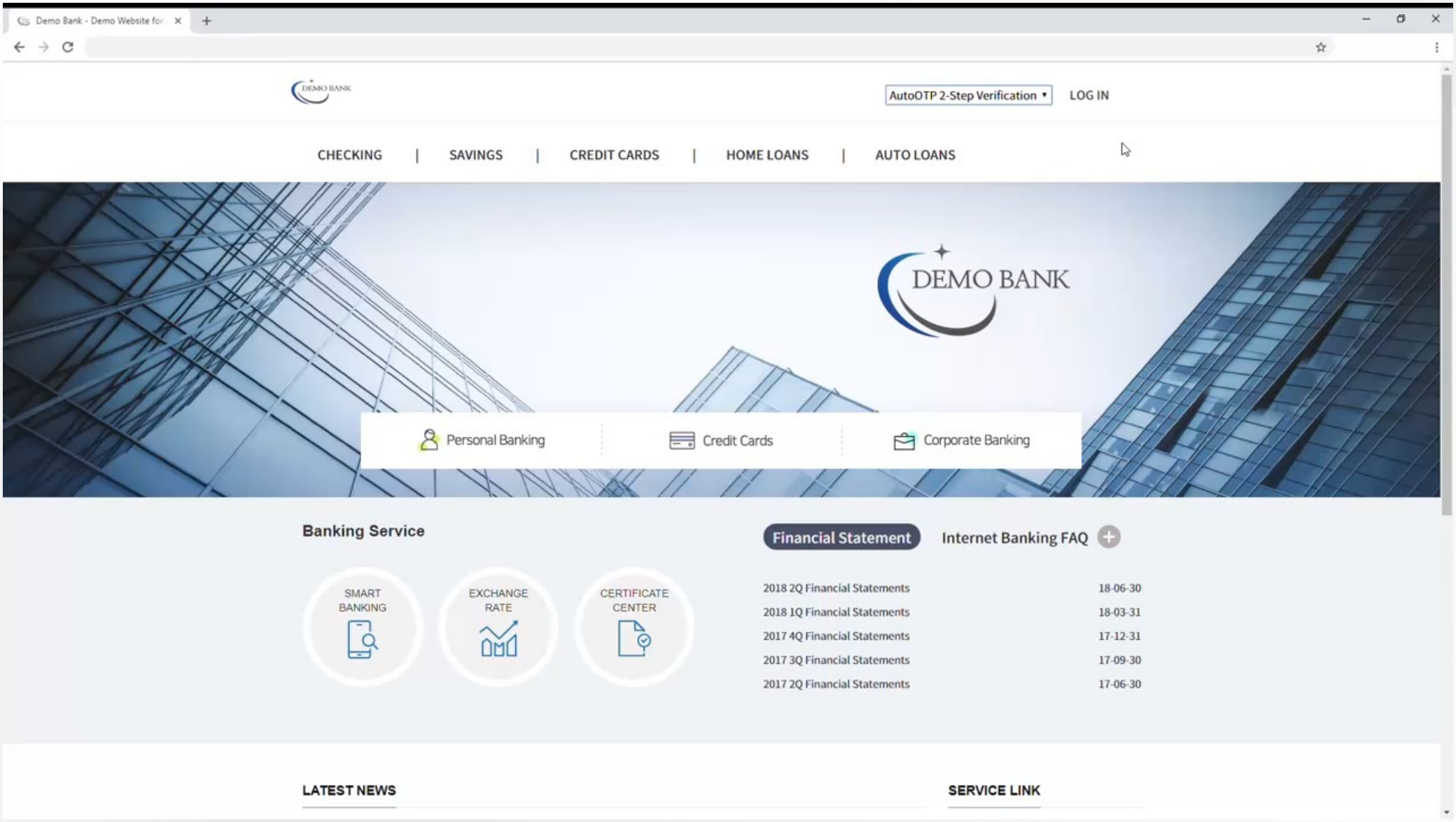
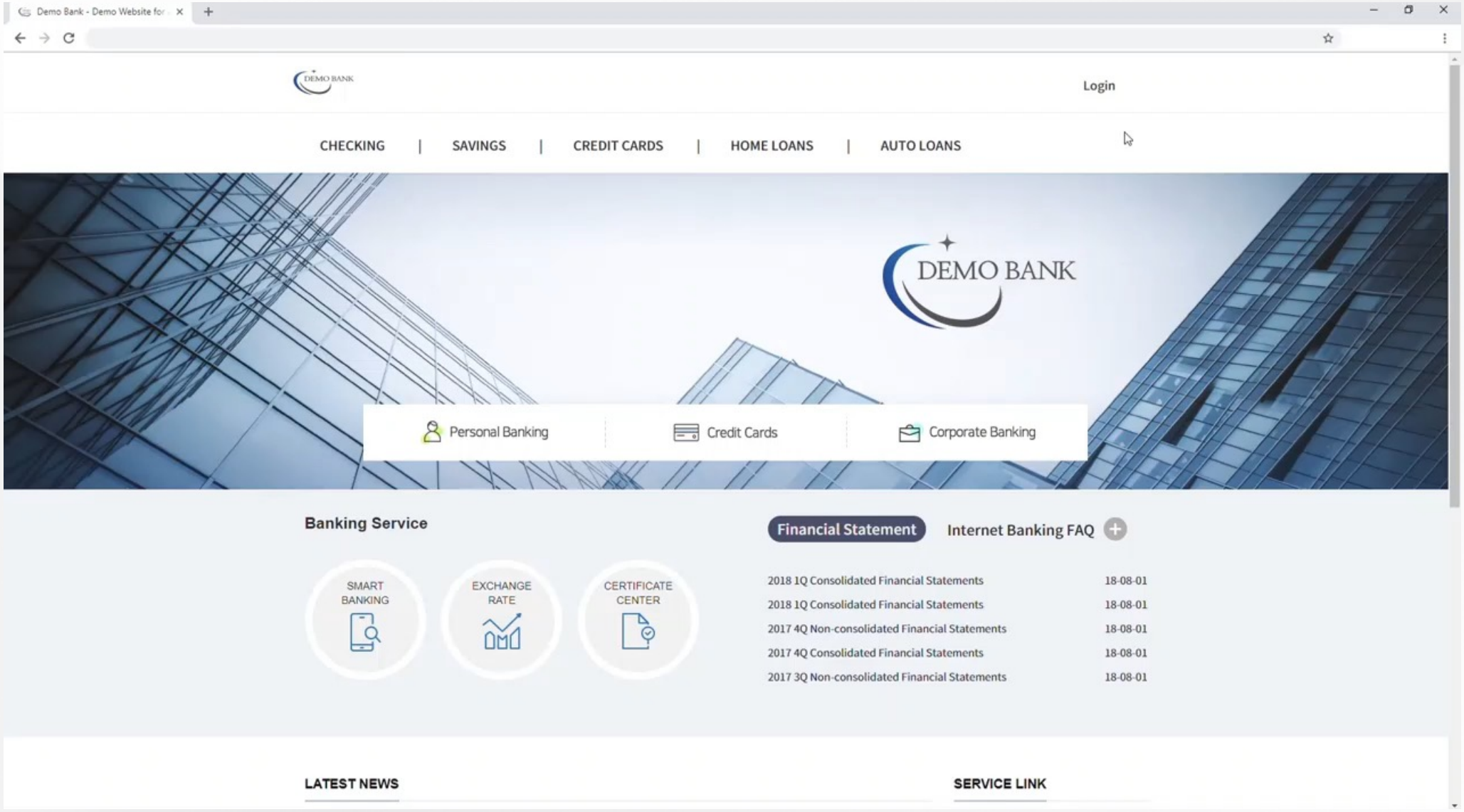
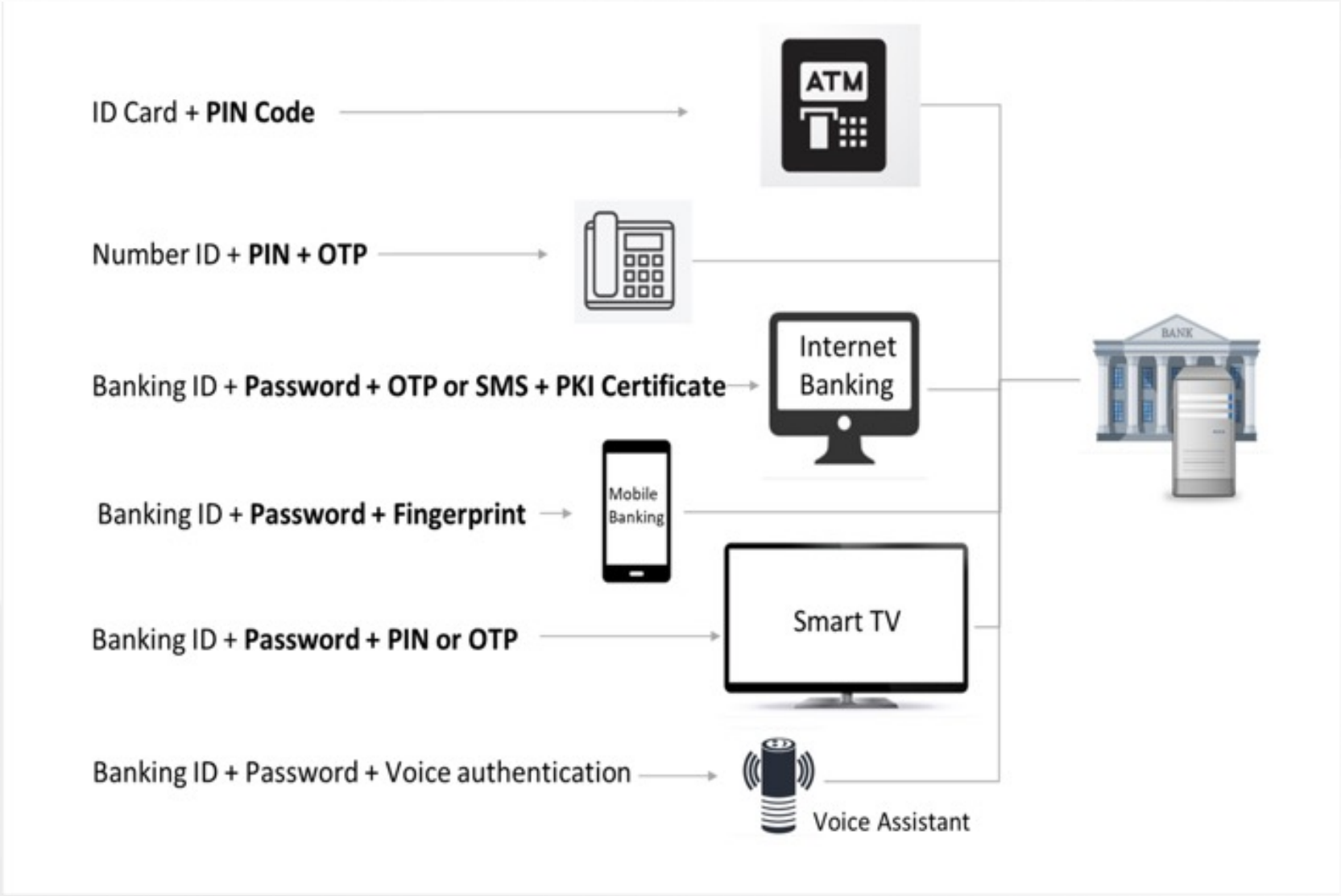
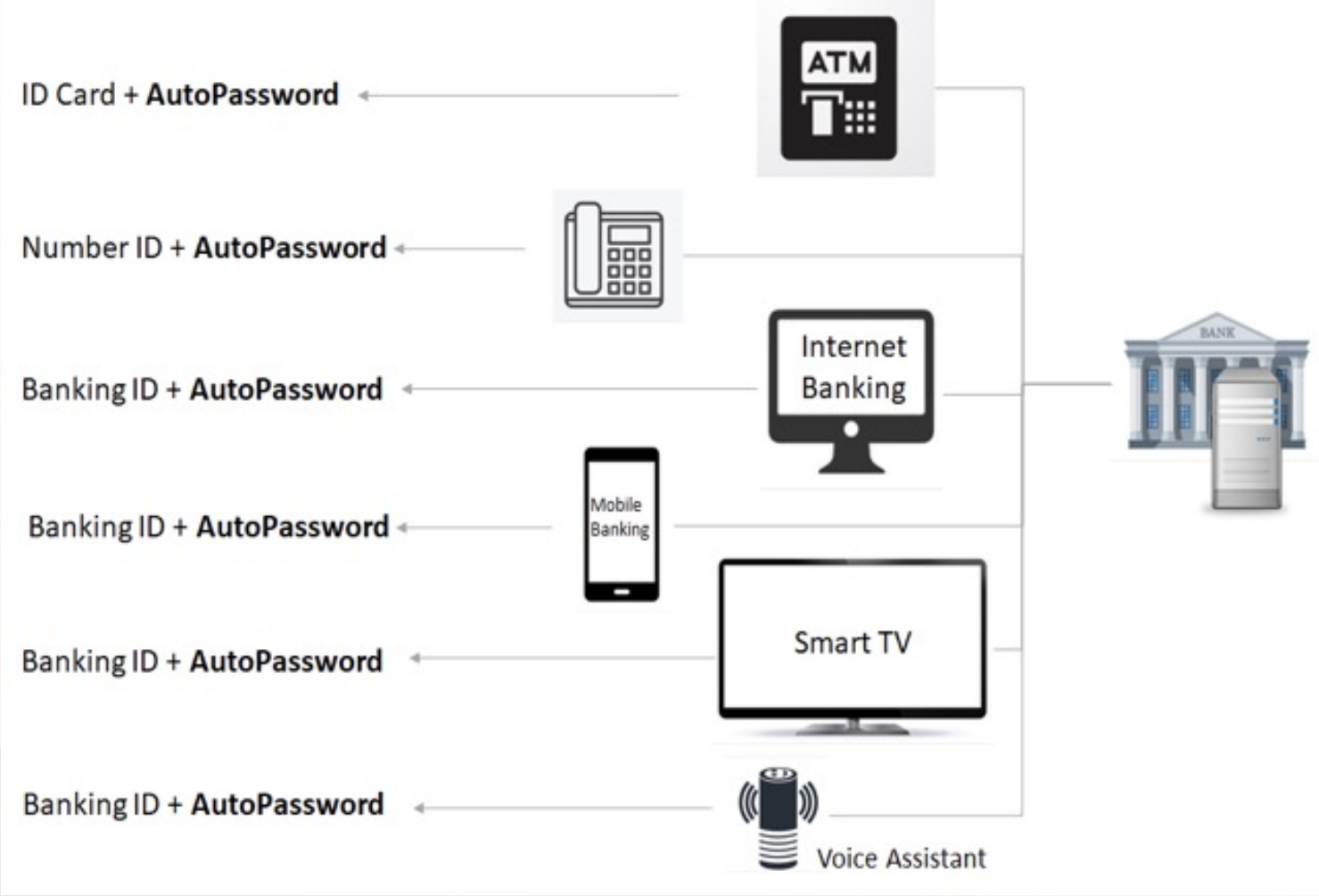

User
User terminal
Relying party
Verifier
Server
authentication information
Server
authentication information
Server
authentication information
Offset for server authentication information generation
Out-of-band
server authenticator

Figure 6 – Example of server verification information presentation


Demo Bank - Demo Website for
DEMO BANK
AutoOTP 2-Step Verification
LOG IN
CHECKING | SAVINGS | CREDIT CARDS | HOME LOANS | AUTO LOANS
DEMO BANK
Personal Banking
Credit Cards
Corporate Banking
Banking Service
SMART BANKING
EXCHANGE RATE
CERTIFICATE CENTER
Financial Statement
Internet Banking FAQ
2018 2Q Financial Statements 18-06-30
2018 1Q Financial Statements 18-03-31
2017 4Q Financial Statements 17-12-31
2017 3Q Financial Statements 17-09-30
2017 2Q Financial Statements 17-06-30
LATEST NEWS
SERVICE LINK


Demo Bank - Demo Website for
DEMO BANK
Login
CHECKING | SAVINGS | CREDIT CARDS | HOME LOANS | AUTO LOANS
DEMO BANK
Personal Banking
Credit Cards
Corporate Banking
Banking Service
SMART BANKING
EXCHANGE RATE
CERTIFICATE CENTER
Financial Statement
Internet Banking FAQ
2018 1Q Consolidated Financial Statements 18-08-01
2018 1Q Consolidated Financial Statements 18-08-01
2017 4Q Non-consolidated Financial Statements 18-08-01
2017 4Q Consolidated Financial Statements 18-08-01
2017 3Q Non-consolidated Financial Statements 18-08-01
LATEST NEWS
SERVICE LINK


ID Card + **PIN Code**
ATM
Number ID + **PIN + OTP**
Banking ID + **Password + OTP or SMS + PKI Certificate**
Internet Banking
Banking ID + **Password + Fingerprint**
Mobile Banking
Banking ID + **Password + PIN or OTP**
Smart TV
Banking ID + Password + Voice authentication
Voice Assistant
BANK


ID Card + **AutoPassword**
Number ID + **AutoPassword**
Banking ID + **AutoPassword**
Banking ID + **AutoPassword**
Banking ID + **AutoPassword**
Banking ID + **AutoPassword**
ATM
Internet Banking
Mobile Banking
Smart TV
Voice Assistant
BANK

W3C Working Group Note

DID Specification Registries

The interoperability registry for Decentralized Identifiers

W3C Working Group Note 02 November 2021

▼ More details about this document

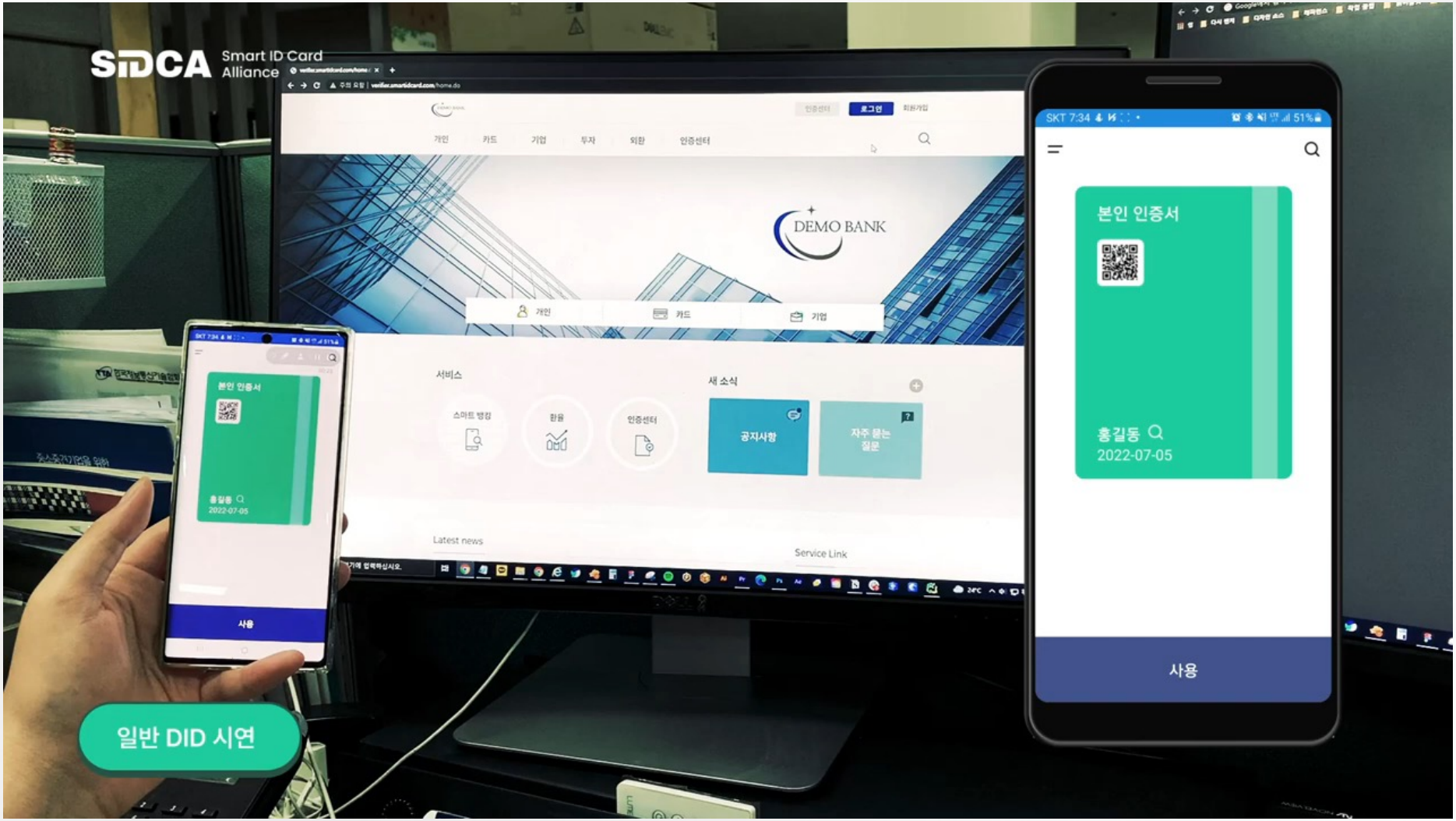
This version:
https://www.w3.org/TR/2021/NOTE-did-spec-registries-20211102/

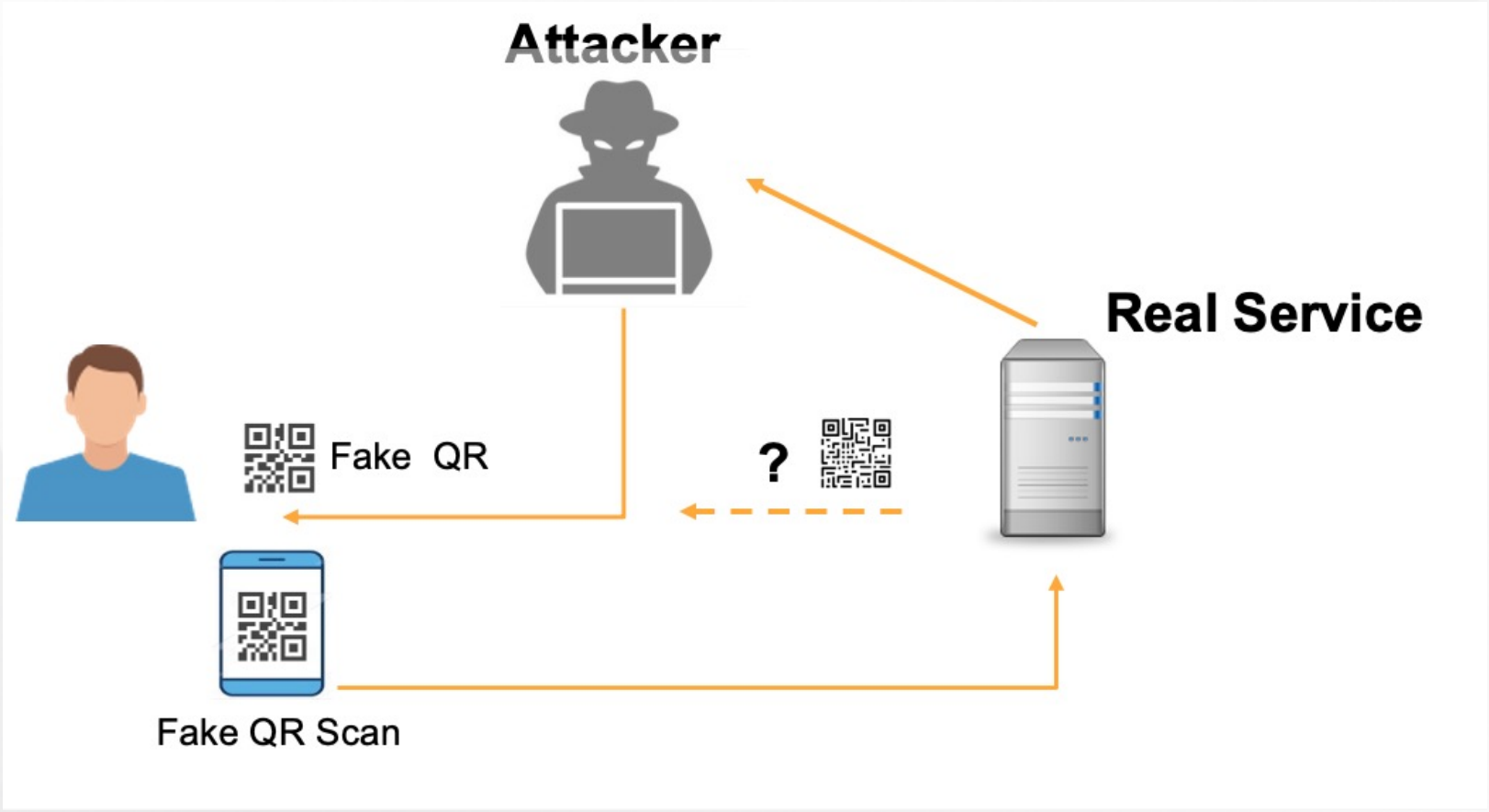
Latest published version:
https://www.w3.org/TR/did-spec-registries/

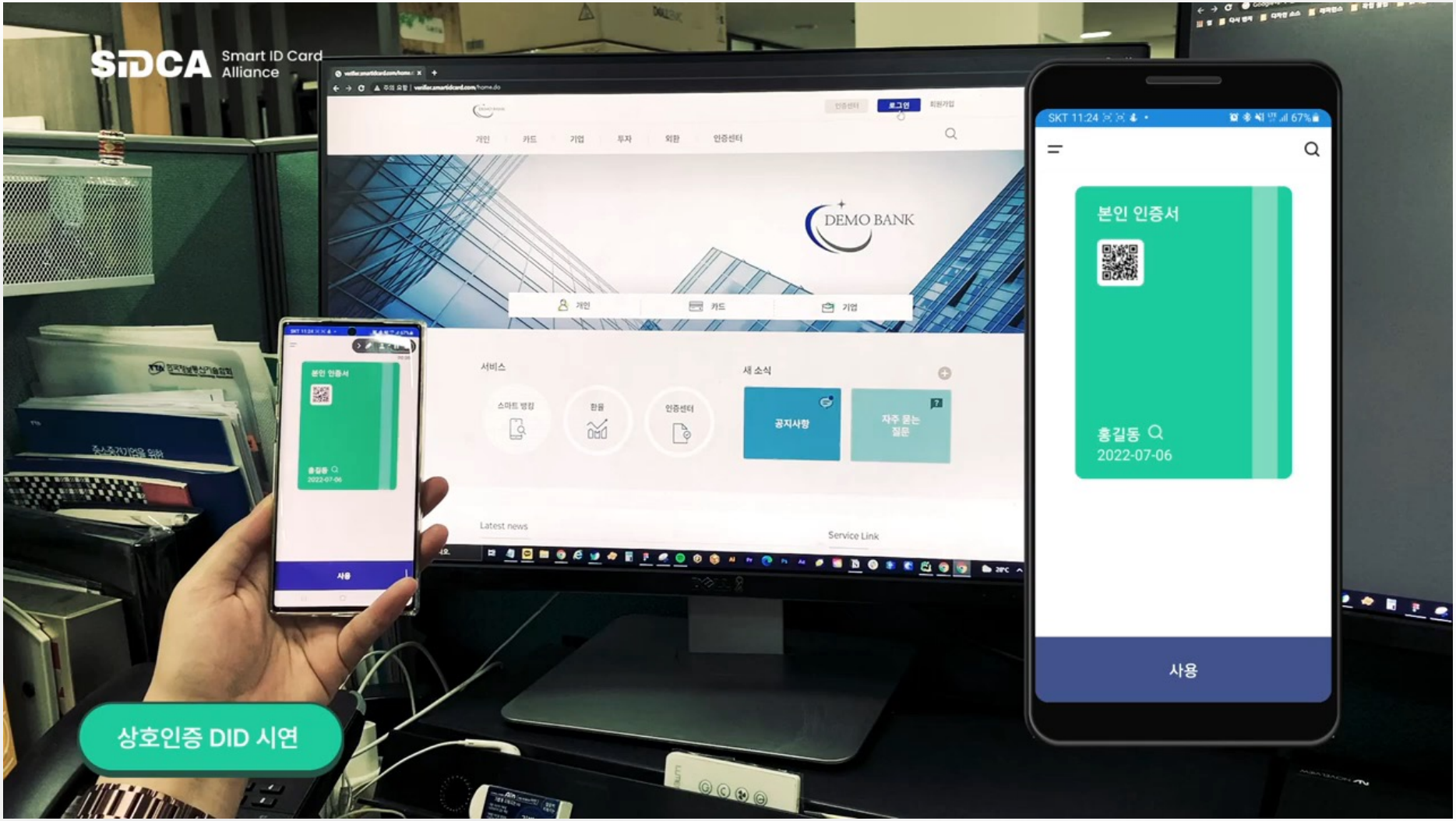
Latest editor's draft:
https://w3c.github.io/did-spec-registries/

History:
Publication history
Commit history

Previous version:


SIDCA Smart ID Card Alliance
DEMO BANK
개인
카드
기업
서비스
새 소식
공지사항
자주 묻는 질문
Latest news
Service Link
본인 인증서
홍길동
2022-07-05
사용
일반 DID 시연


Attacker
Real Service
Fake QR
?
Fake QR Scan


SIDCA Smart ID Card Alliance
DEMO BANK
서비스
새 소식
공지사항
자주 묻는 질문
Latest news
Service Link
SKT 11:24
본인 인증서
홍길동
2022-07-06
사용
상호인증 DID 시연

Out of Band Authentication with AAL3

Offline IoT Service

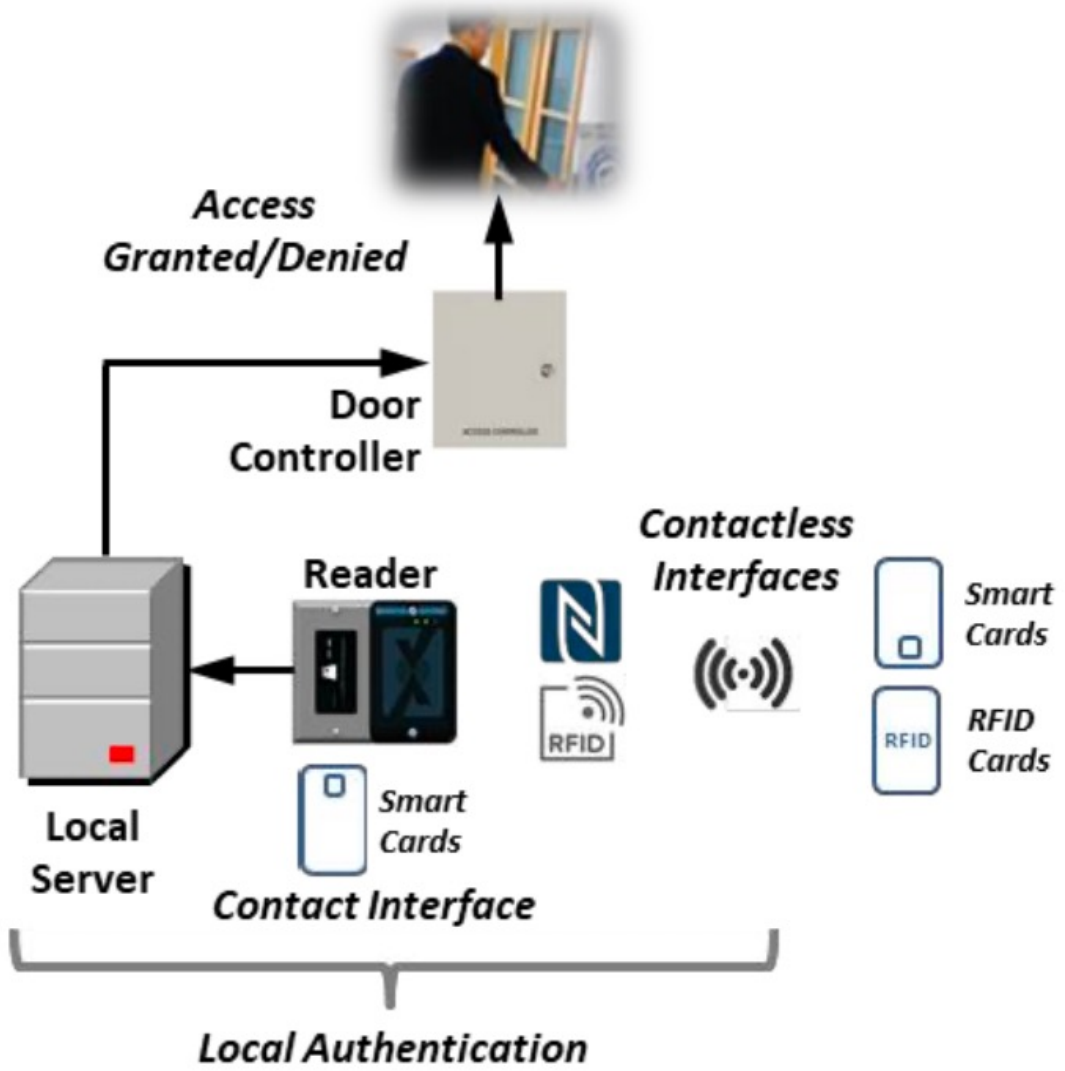
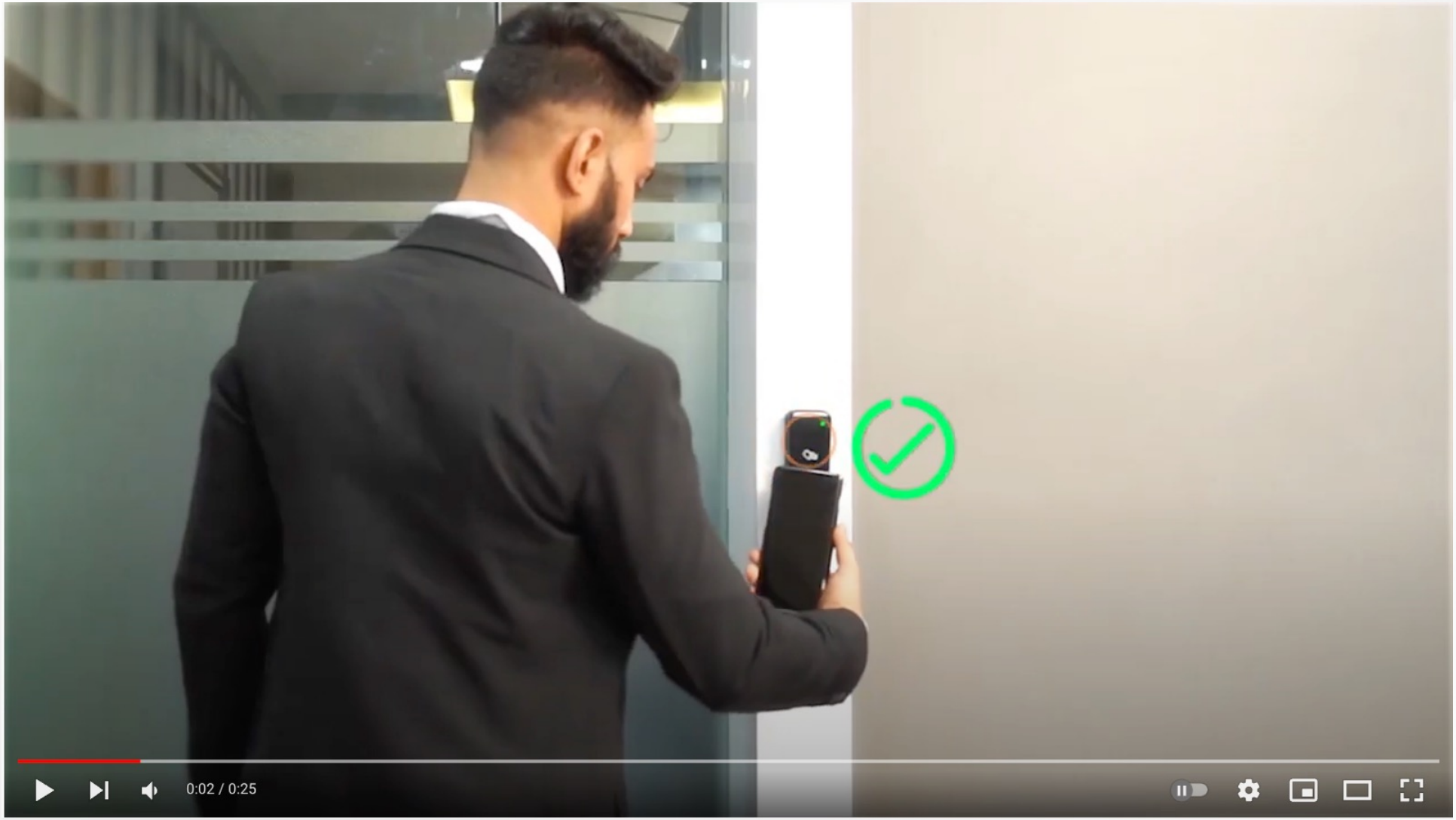
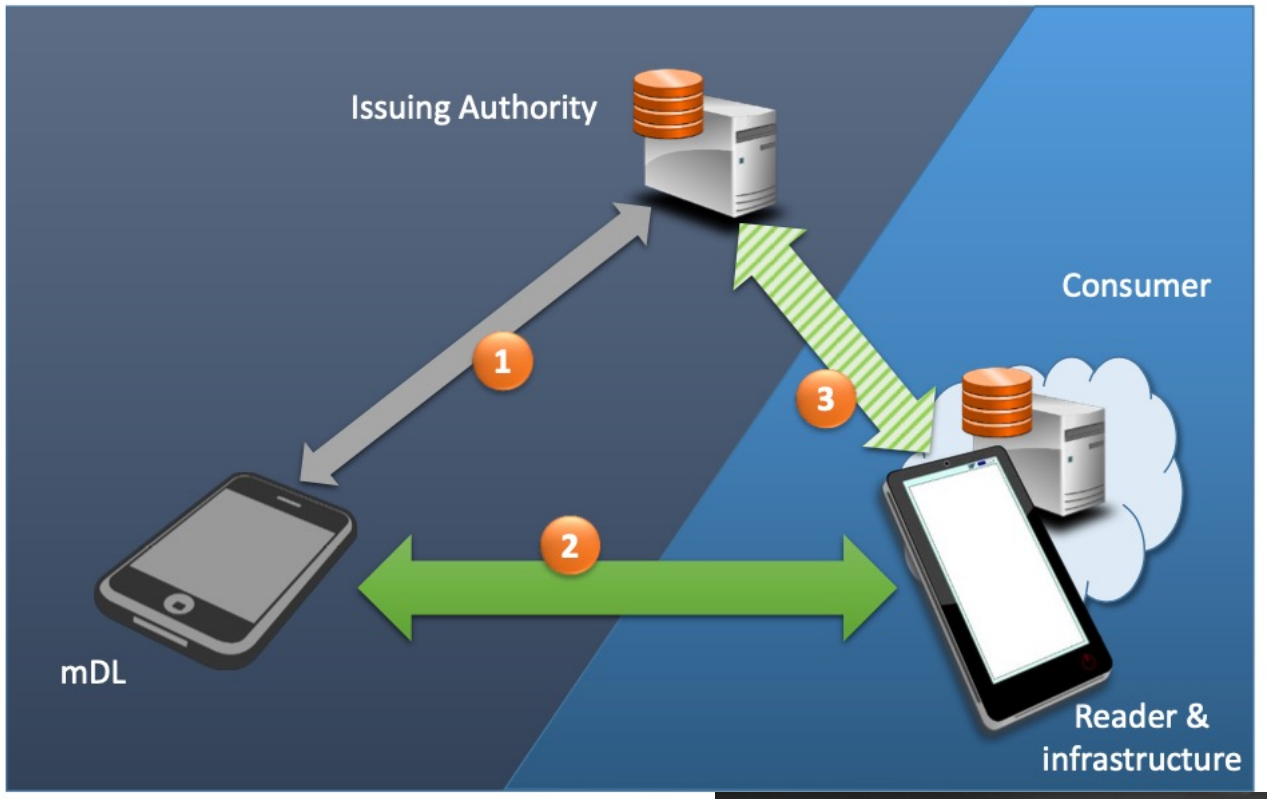


Figure 8. Traditional Relying Party PACS Architecture



https://youtu.be/o0FUh90sp4Y


Issuing Authority
Consumer
1
2
3
mDL
Reader &
infrastructure


⑤ 면허정보&개인키
단말 내 저장
⑥ 모바일 운전면허증
등록 완료
위변조/탈취 불가능
(Keystore/Keychain/USIM)
모바일 운전면허증
등록 정보 암호화
사용자
검증앱
구동
검증자
홍길동
검증결과 확인
Valid
Invalid

< 진위확인 절차 >

가정

사용자 인증값을 읽는 서비스 제공자가 정당하다

Remote authentication

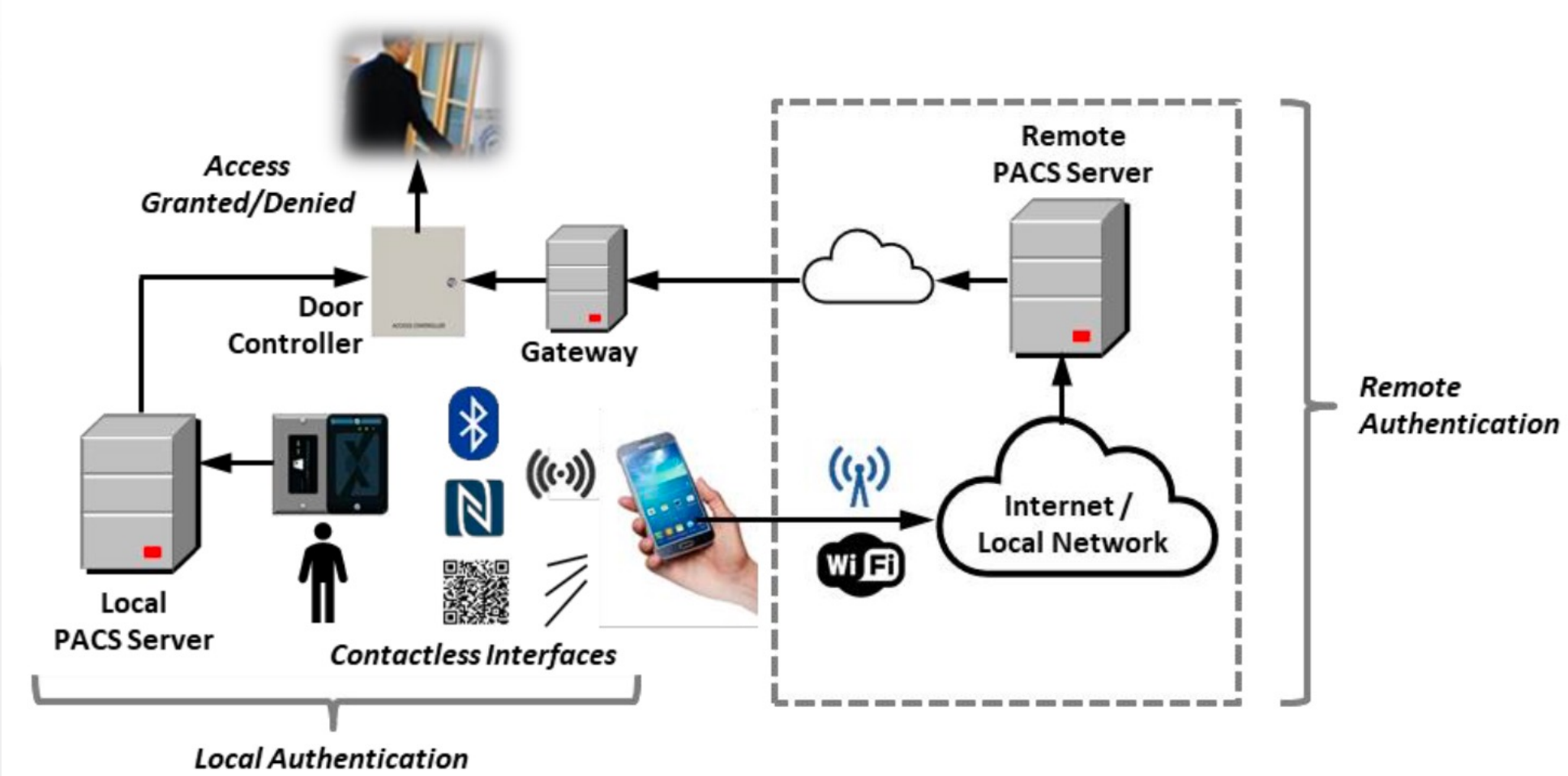
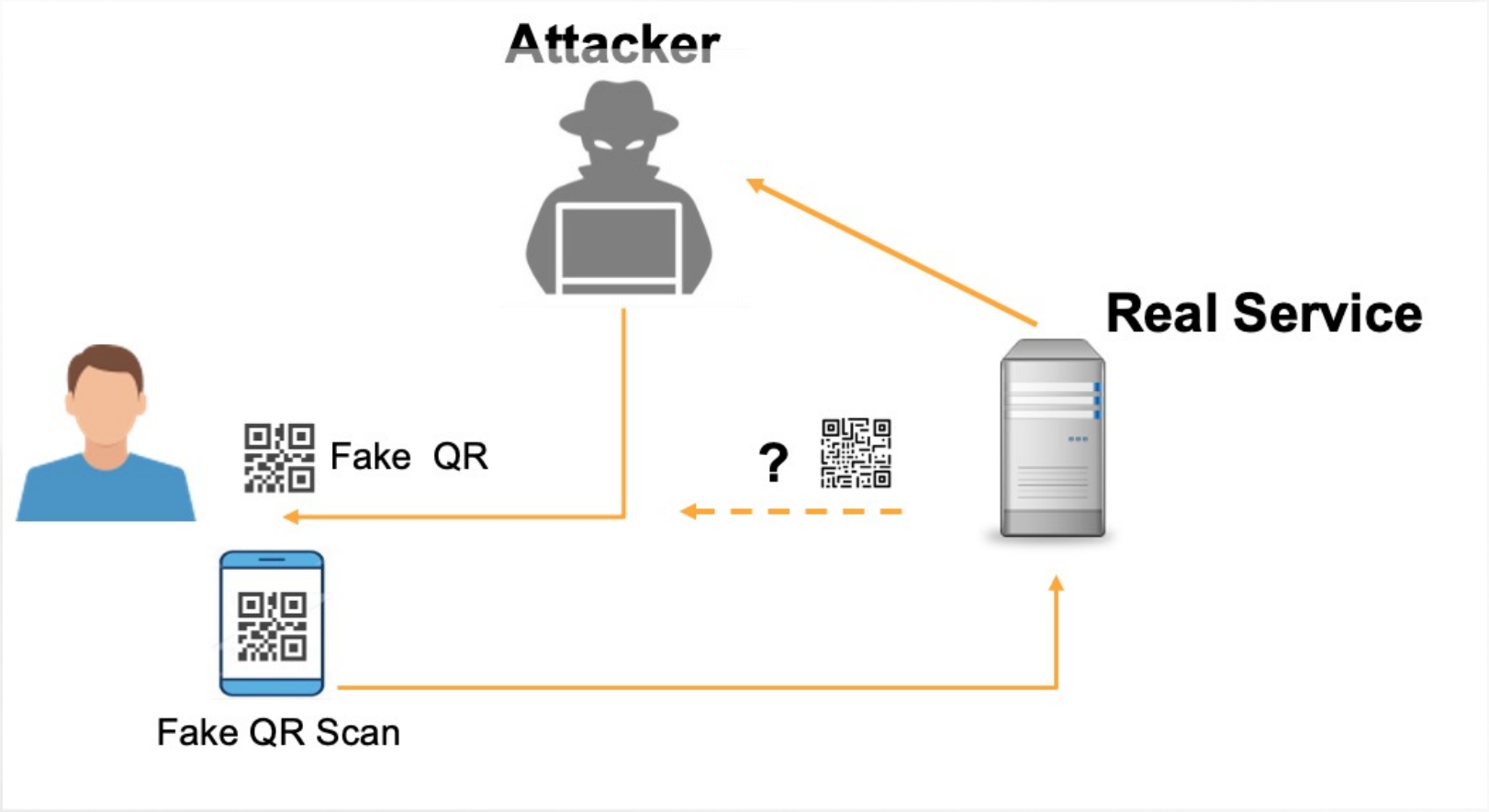


Figure 9. Mobile-Enabled PACS Relying Party Architecture

가정

서비스 제공자가 내가 인증한 정당한 서비스 제공자


Attacker
Real Service
Fake QR
?
Fake QR Scan

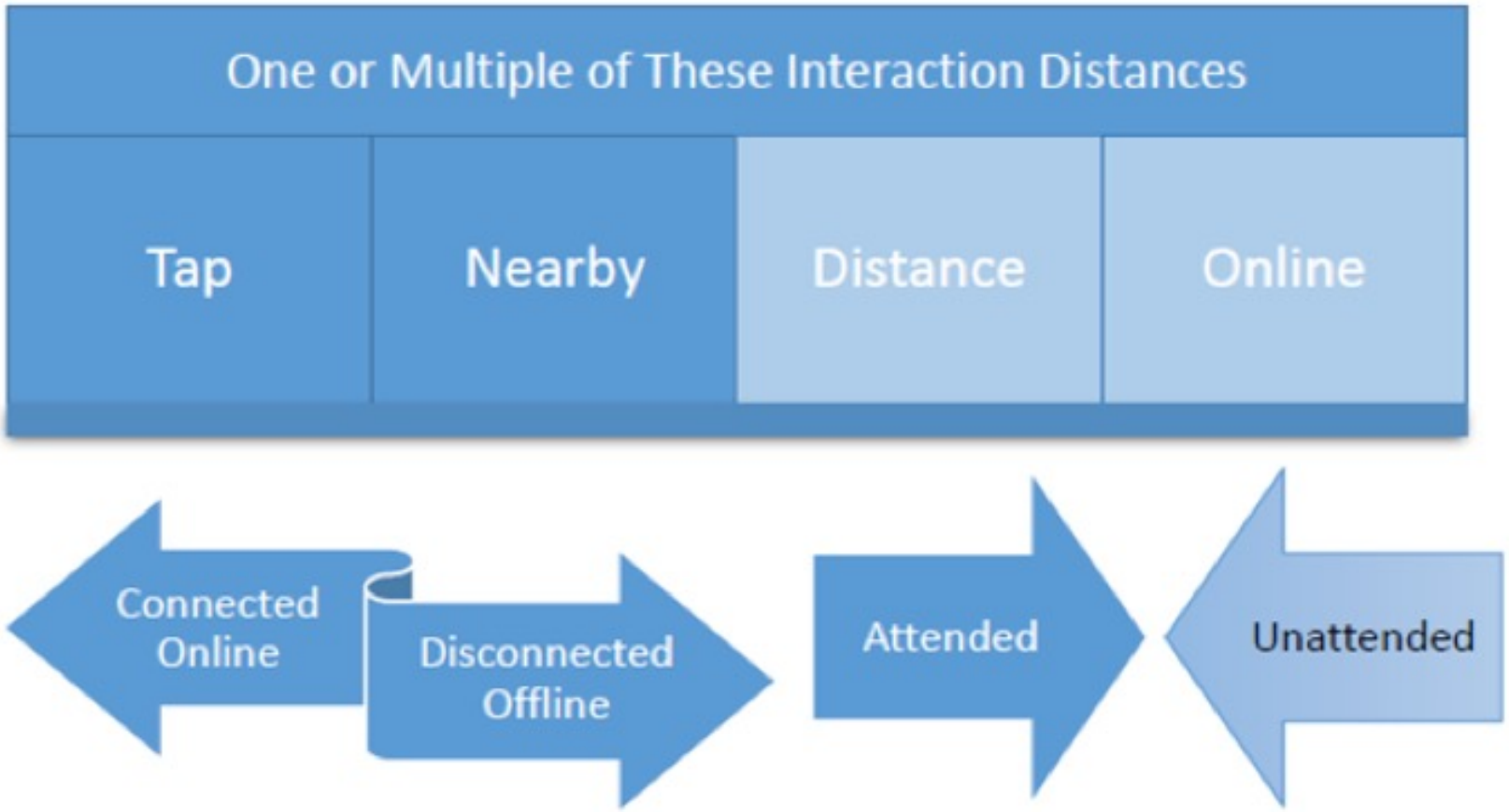


Figure 4. Possibilities/Variables that Verifiers Consider that Create Interaction Modes (Lighter blue are Day Two interactions)

< mDL 운영 방식: Day 1, Day 2 >

구분	Day 1 기능 유인/대면 처리 과정	Day 2 기능 무인/비대면 및 온라인 처리 과정
연결	서비스 보유자가 서비스 검증자를 대면한 상태에서 정보 제공 동의로 QR 코드를 제시하거나 NFC를 태그한다.	서비스 보유자가 서비스 검증자를 원거리 대면한 상태에서 정보 제공 동의로 NFC를 태그하거나 블루투스 비콘을 선택한다.
전송	NFC, 블루투스, Wi-Fi Aware 를 사용하여 근접 거리 및 근거리 데이터 전송 인터넷에 연결된 상태에서는 빠른 처리를 위해 온라인 검색	원거리 전송을 위해 웹 서비스 추가 육안으로 검증자가 확인이 안 될 때 소지자를 악성 리더기(검증자)로부터 보호해야함.
신원 확인	근거리에서 검증자가 직접 소지자 실물과 수신한 사진을 비교	사진 없이 자동화된 신원 인증을 위한 대면 또는 원거리 소지자 인증 육안으로 검증자가 확인이 안 될 때, 소지자는 검증자에게 정보를 공유하기 전 검증자의 리더기를 확인해야함

언택트 방문증 정보통신단체표준 기술

TTA Standard

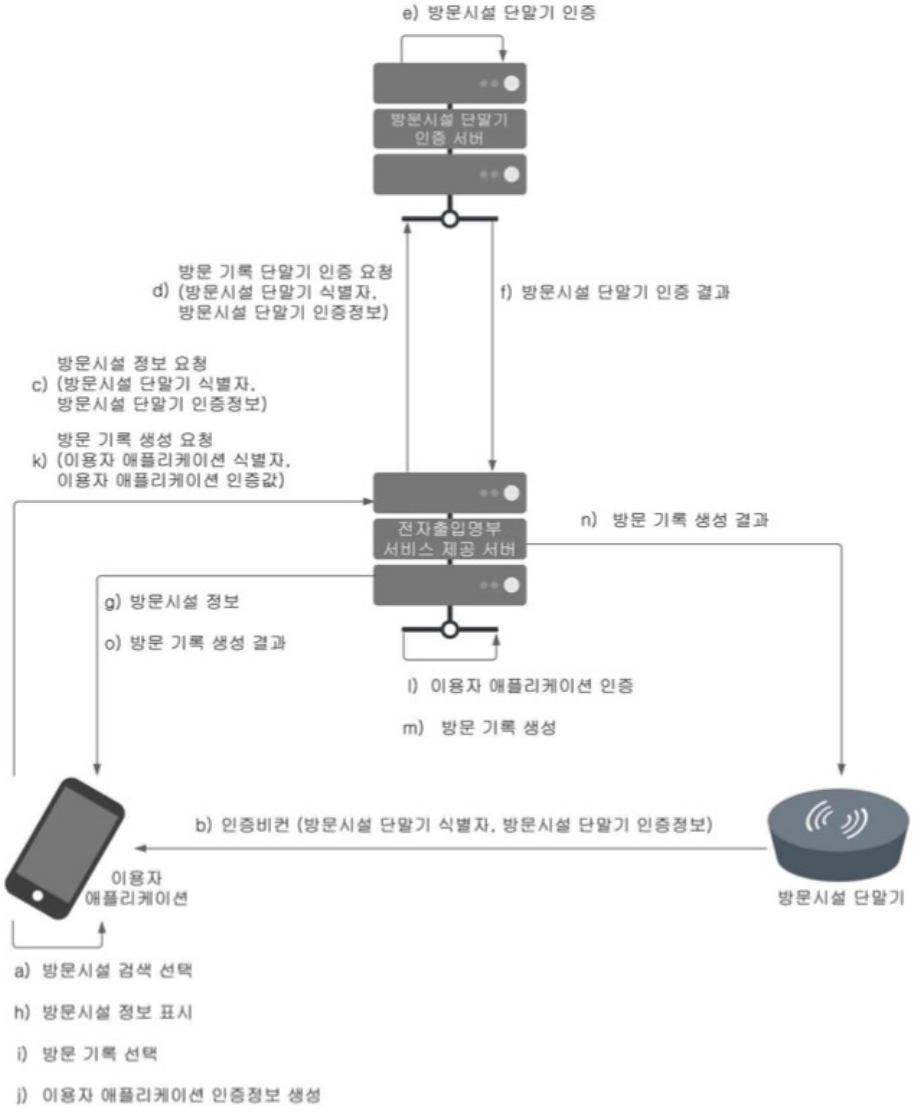
정보통신단체표준(국문표준)

TTAK.KO-12.0369 제정일: 2021년 6월 30일

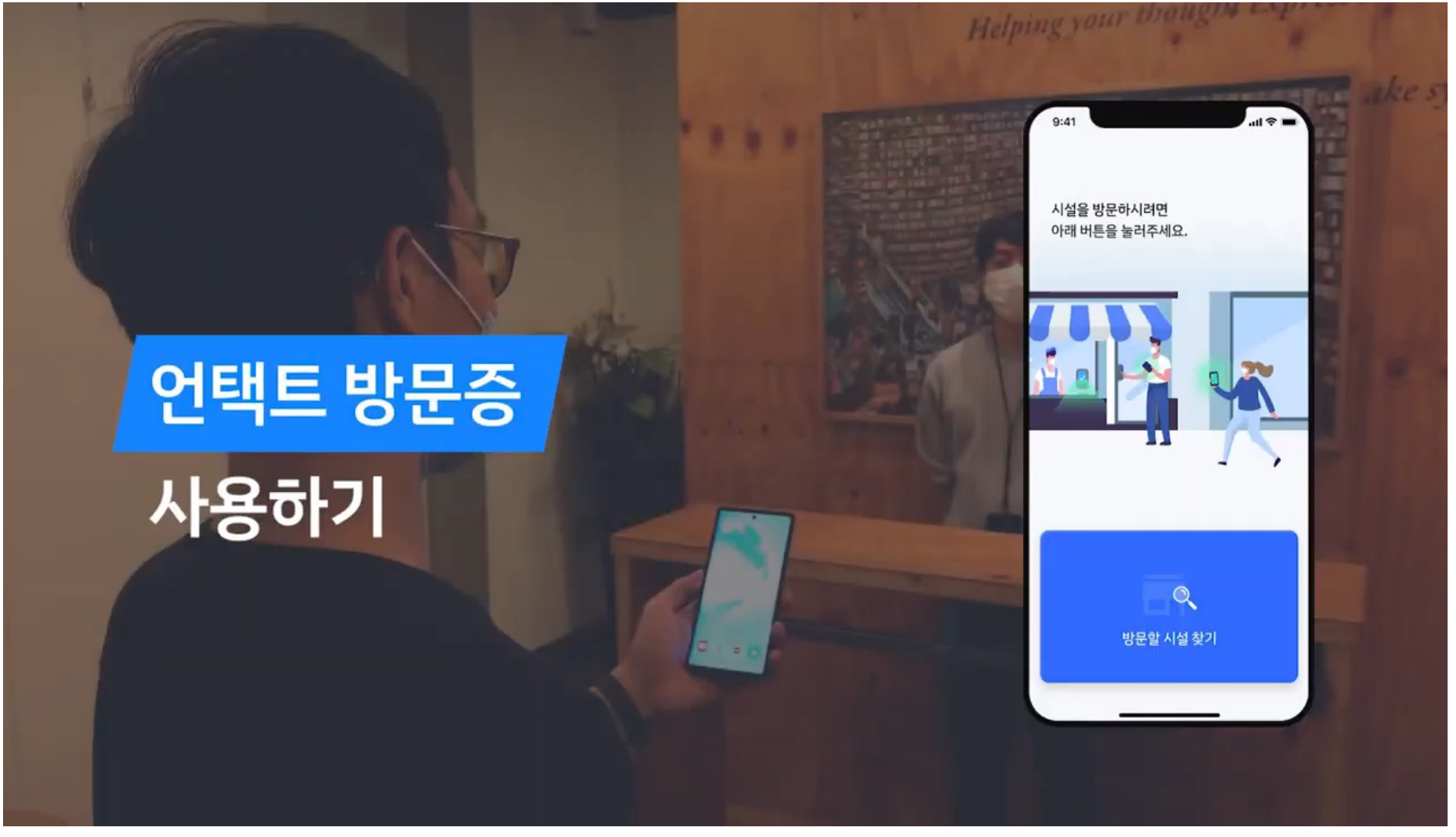
비컨 기반 동적 인증정보를 이용한
전자출입명부 기록 절차

Digital Entry Logging Procedures Using
Beacon-Based Dynamic Authentication Information

TTA 한국정보통신기술협회
Telecommunications Technology Association



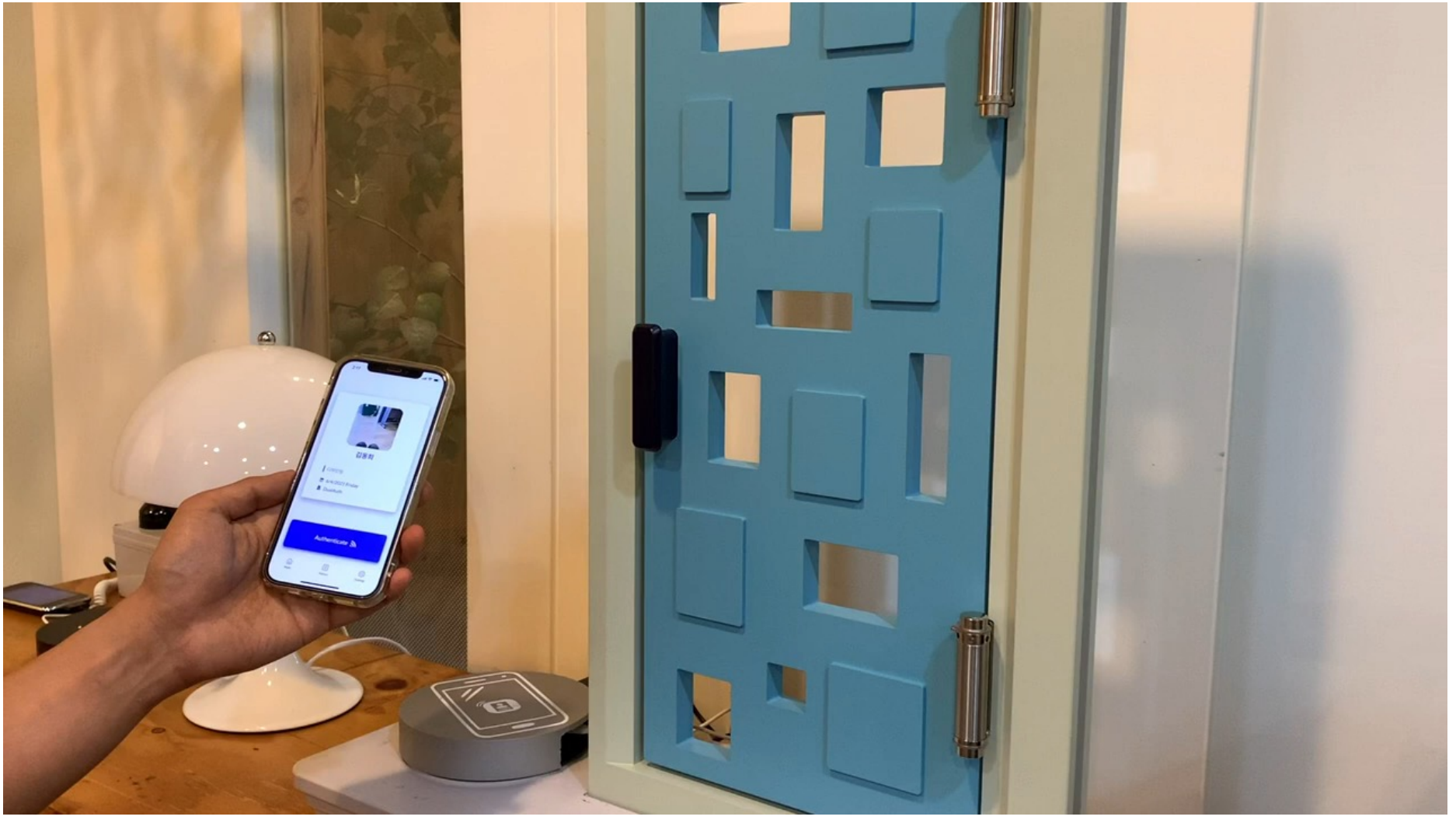
언택트방문증 시연 영상



영상이 재생되지 않는 경우 유튜브 링크로 접속하세요.
https://youtu.be/qJwQ1tHKulQ

6.3 주요 결과물 (인증비컨 기반 전기제어 동영상)

6.3 주요 결과물 (인증비컨 기반 출입문 제어 동영상)



DualAuth

01

소개

02

IoT 보안 사고와 인증 기술 유형

03

IoT 서비스 인증 기술 요건 및 표준화 동향

04

요약

04 요약

IoT 서비스에서의 고려해야할 인증 기술 (보안성, 사용성, 경제성)

인증 기술은 적은 비용으로 IoT의 보안을 크게 개선

생체인증, 블록체인기반 DID 인증, 모바일 운전면허 사용자 인증 흐름 등 조사

인증기술 구분 방법 (In Band vs Out of band, Local vs Remote, AAL)

IoT 서비스에 대한 인증 기술 요건 (On/Offline)

Online Authentication 동향

Offline Authentication 동향

DualAuth

감사합니다.