글로벌 ICT 표준 컨퍼런스 2023
Global ICT Standards Conference 2023

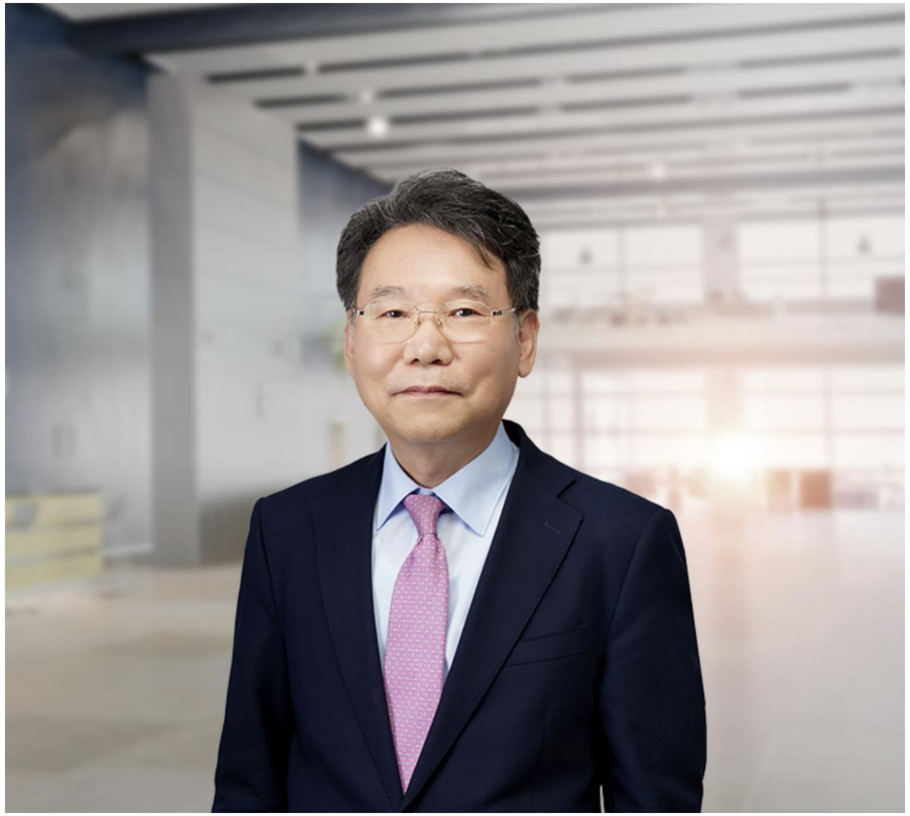
(세션7) ICT 표준화 전략 및 활동 지원

ITU-T SG 17 (사이버보안 기술 국제표준) TTA 명장급 멘토링 사례

고형승 미국변호사(팀장), (주)에프엔에스벨류

주최 과학기술정보통신부 Ministry of Science and ICT 특허청 Korean Intellectual Property Office
주관 국립전파연구원 National Radio Research Agency TTA IITP KEA kista ETRI

01. 멘토 소개 및 약력



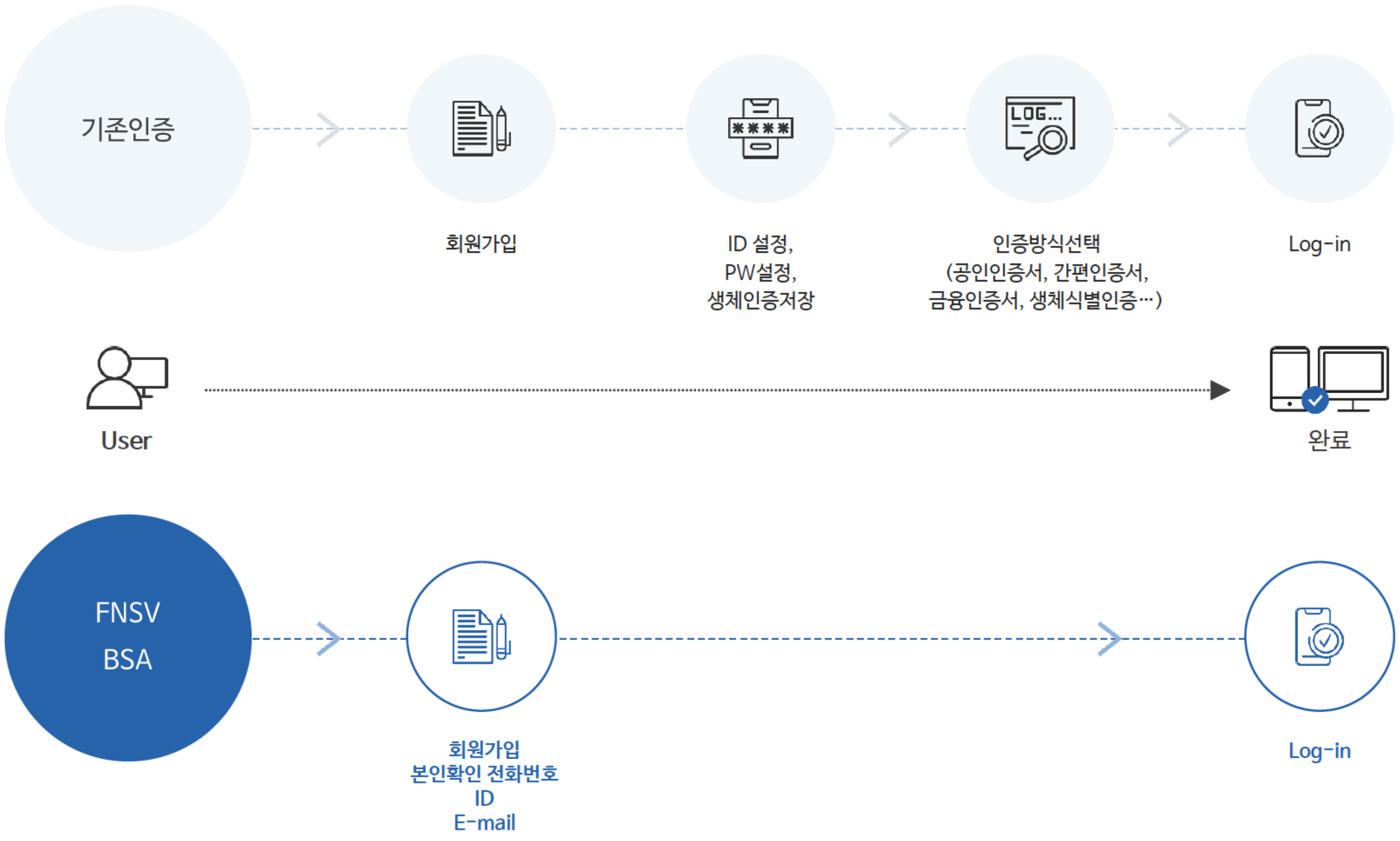
순천향대학교 염흥열 교수님

학력
한양대학교 전자공학과 학사
한양대학교 대학원 전자공학과 석사
한양대학교 대학원 전자공학과 박사

경력

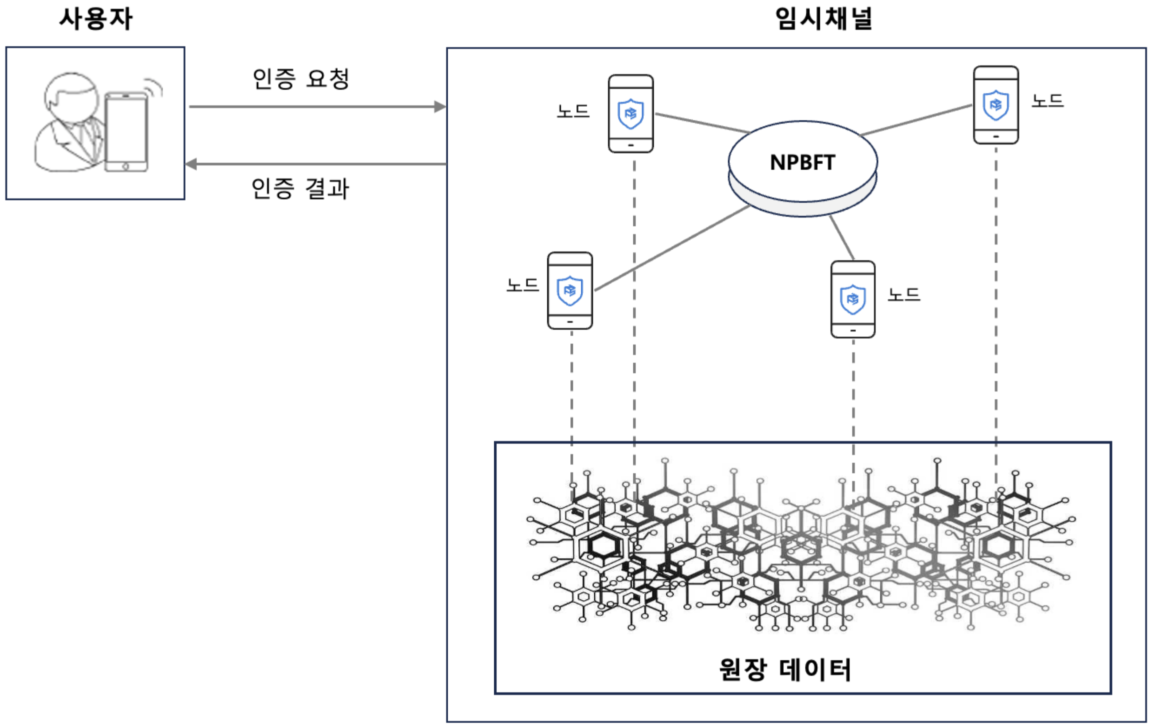
2007.03 - 현재	한국인터넷진흥원 ISMS/PIMS 인증위원회 위원장
2012.01 - 현재	한국정보보호학회 명예회장
2013.12 - 현재	순천향대학교 SCH사이버보안연구센터 센터장
2016.10 - 현재	ITU-T SG17 의장
2019.05 - 현재	과학기술정보통신부 정보통신기술 국제표준 마에스트로
2019.10 - 2022.04	대통령실 국가안보실 정책자문위 위원
2020.08 - 2023.08	개인정보보호위원회 위원 (차관급)

02. Blockchain Secure Authentication (BSA)

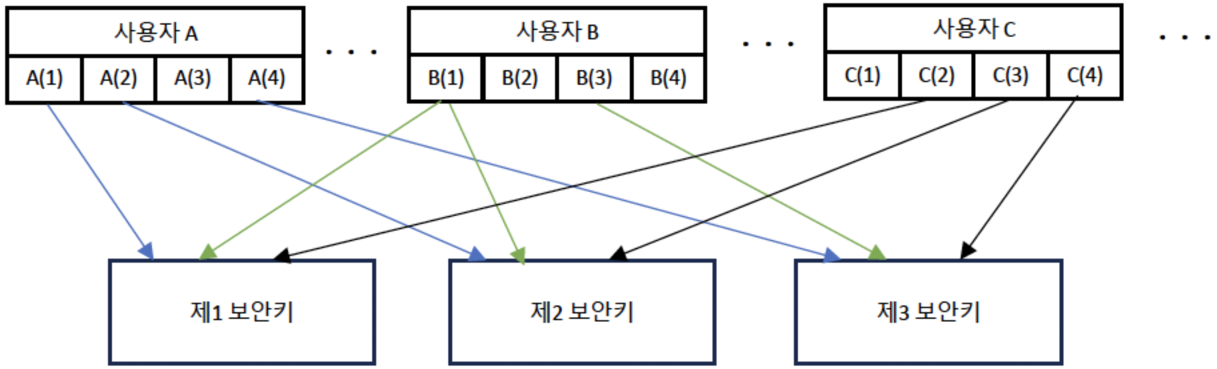


03. Blockchain Secure Authentication (BSA)

1. 블록체인 기술을 이용한 사용자 기기 인증



2. 분산원장 내 사용자 정보 조합을 통한 일회성 인증키 생성



04. BSA 효과 및 활용 범위

[BSA 효과]

- 패스워드리스 인증 구현
- 비밀 번호 등 인증에 필요한 정보•기기 관리의 어려움 해소
- 계정 탈취 및 데이터 침해 위험 감소
- 신속•정확한 인증으로 사용자 편의성 증대

[BSA 활용 범위]

- 사용자 계정 인증이 필요한 서비스
  - 기업, 금융, 유통 등의 계정 서비스 인증
  - 웹•모바일 애플리케이션 사용자 인증
  - 고객, 사용자 신원확인 서비스
- 개인정보 도용 위험 없는 앱카드
- 가상자산 보관에 대한 인증, 토큰 교환 및 암호화폐거래소 (Wallet Server), 탈중앙거래소 (DEX, DEXes) 서비스
- 커넥티드 카 (Connected Car)

05. ITU & FNSValue 파트너십

Strong Passwordless Blockchain Authentication
ITU & FNSValue Partnership Launch Ceremony
fnsvalue

ITU & FNSV Partnership Launch Ceremony

ITURDF
ASIA-PACIFIC REGION
BANGKOK 2023
Post-Session: Digital Financial Services (DFS) Security Clinic

DFS Security Clinic in Bangkok

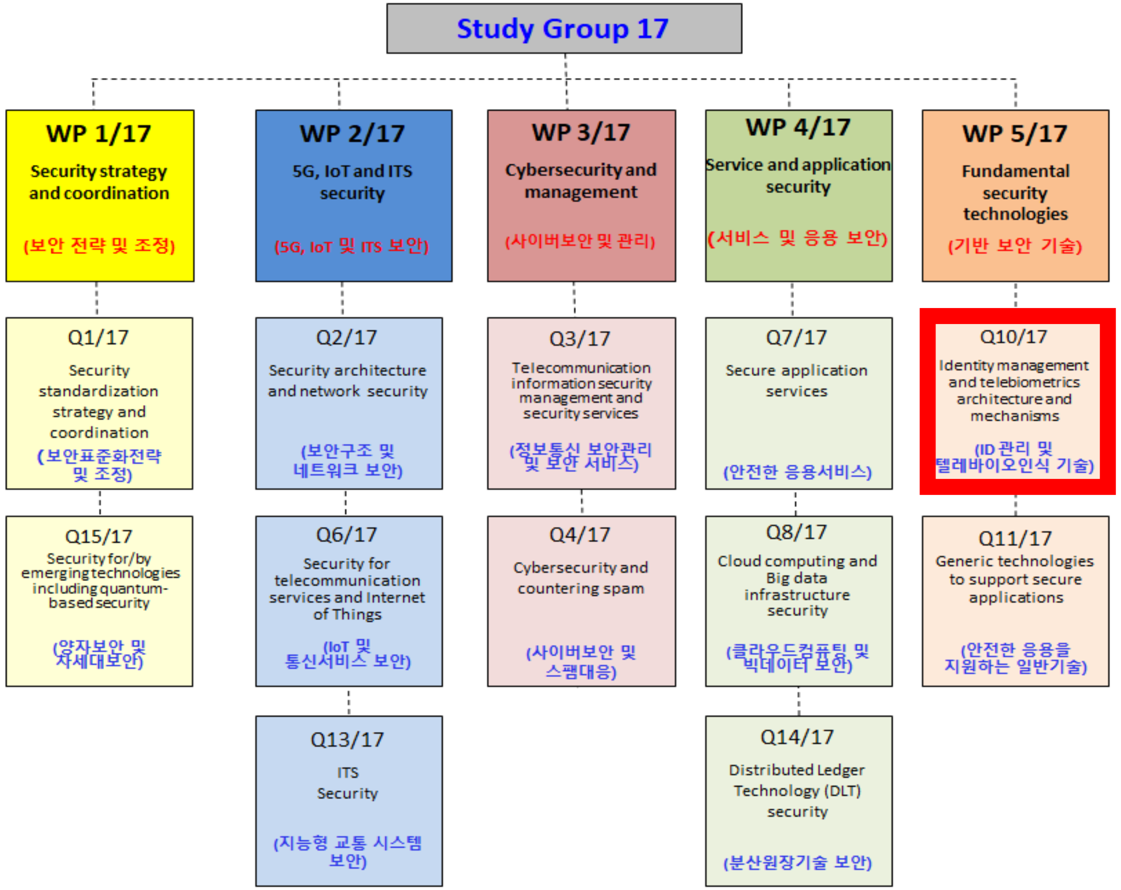
06. ITU-T Study Group17 Meeting

대한민국, 고양시, 2023년 8월 29일 – 9월 8일

ITU
ITU-T Study Group 17 Korea 2023
ITU-T Study Group 17 Korea 2023
29 August – 8 September 2023 | Goyang, Korea (Republic of)
GrandBallroomA

07. ITU-T Study Group17

ITU-T SG17, Security (정보보호)



Study Group 17

WP 1/17
Security strategy and coordination
(보안 전략 및 조정)

WP 2/17
5G, IoT and ITS security
(5G, IoT 및 ITS 보안)

WP 3/17
Cybersecurity and management
(사이버보안 및 관리)

WP 4/17
Service and application security
(서비스 및 응용 보안)

WP 5/17
Fundamental security technologies
(기반 보안 기술)

Q1/17
Security standardization strategy and coordination
(보안표준화전략 및 조정)

Q15/17
Security for/by emerging technologies including quantum-based security
(양자보안 및 차세대보안)

Q2/17
Security architecture and network security
(보안구조 및 네트워크 보안)

Q6/17
Security for telecommunication services and Internet of Things
(IoT 및 통신서비스 보안)

Q13/17
ITS Security
(지능형 교통 시스템 보안)

Q3/17
Telecommunication information security management and security services
(정보통신 보안관리 및 보안 서비스)

Q4/17
Cybersecurity and countering spam
(사이버보안 및 스팸대응)

Q7/17
Secure application services
(안전한 응용서비스)

Q8/17
Cloud computing and Big data infrastructure security
(클라우드컴퓨팅 및 빅데이터 보안)

Q14/17
Distributed Ledger Technology (DLT) security
(분산원장기술 보안)

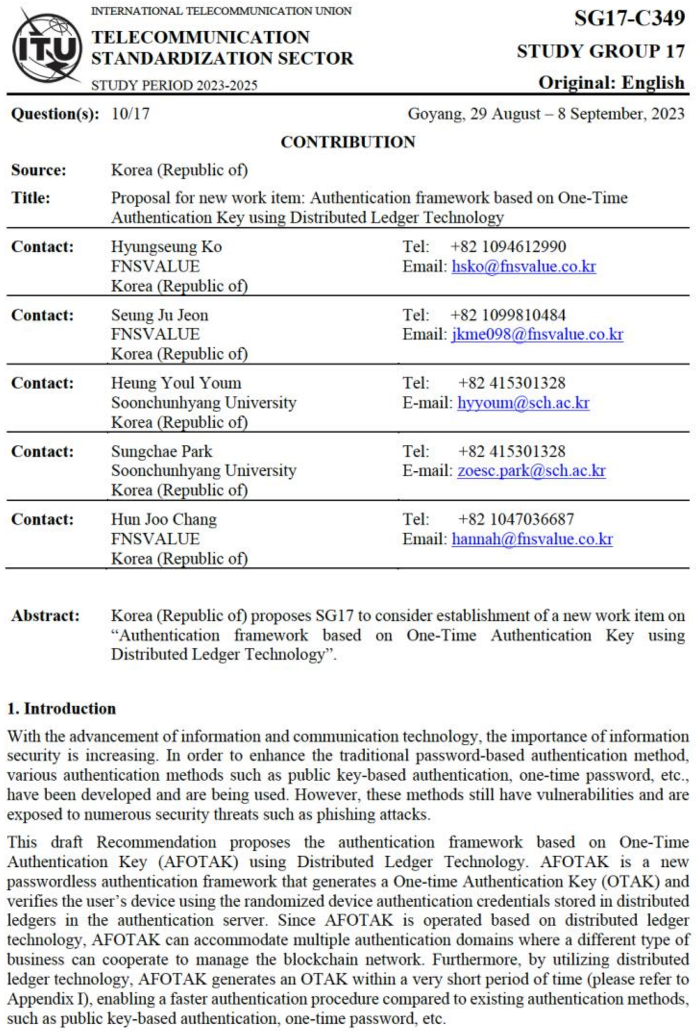
Q10/17
Identity management and telebiometrics architecture and mechanisms
(ID 관리 및 텔레바이오인식 기술)

Q11/17
Generic technologies to support secure applications
(안전한 응용을 지원하는 일반기술)

- ITU-T Study Group 17
- Working Party 5, Question 10
- Q10 Questions

  - t) How can authentication be performed without shared secrets?

08. 멘토링 주요 내용 및 성과



INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2023-2025

SG17-C349
STUDY GROUP 17
Original: English

Question(s):	10/17	Goyang, 29 August – 8 September, 2023

CONTRIBUTION

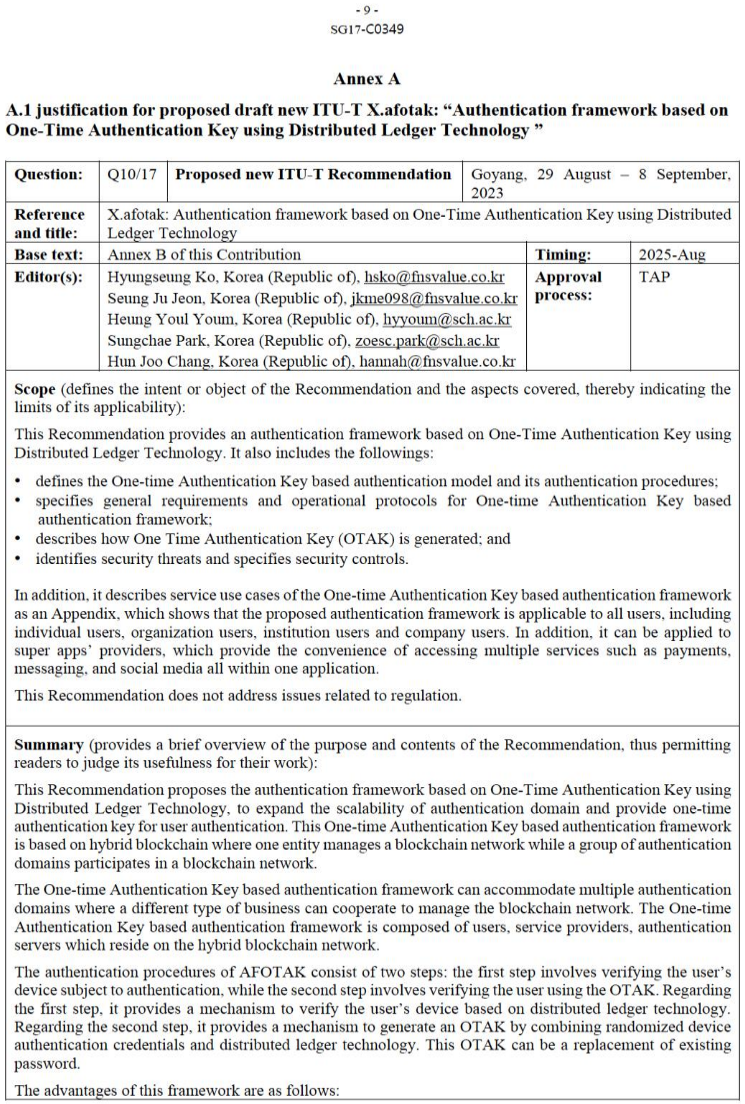
Source:	Korea (Republic of)	
Title:	Proposal for new work item: Authentication framework based on One-Time Authentication Key using Distributed Ledger Technology	
Contact:	Hyungseung Ko FNSVALUE Korea (Republic of)	Tel: +82 1094612990 Email: hsko@fnsvalue.co.kr
Contact:	Seung Ju Jeon FNSVALUE Korea (Republic of)	Tel: +82 1099810484 Email: jkme098@fnsvalue.co.kr
Contact:	Heung Youl Youm Soonchunhyang University Korea (Republic of)	Tel: +82 415301328 E-mail: hyyoum@sch.ac.kr
Contact:	Sungchae Park Soonchunhyang University Korea (Republic of)	Tel: +82 415301328 E-mail: zoesc.park@sch.ac.kr
Contact:	Hun Joo Chang FNSVALUE Korea (Republic of)	Tel: +82 1047036687 Email: hannah@fnsvalue.co.kr

Abstract: Korea (Republic of) proposes SG17 to consider establishment of a new work item on "Authentication framework based on One-Time Authentication Key using Distributed Ledger Technology".

1. Introduction

With the advancement of information and communication technology, the importance of information security is increasing. In order to enhance the traditional password-based authentication method, various authentication methods such as public key-based authentication, one-time password, etc., have been developed and are being used. However, these methods still have vulnerabilities and are exposed to numerous security threats such as phishing attacks.

This draft Recommendation proposes the authentication framework based on One-Time Authentication Key (AFOTAK) using Distributed Ledger Technology. AFOTAK is a new passwordless authentication framework that generates a One-time Authentication Key (OTAK) and verifies the user's device using the randomized device authentication credentials stored in distributed ledgers in the authentication server. Since AFOTAK is operated based on distributed ledger technology, AFOTAK can accommodate multiple authentication domains where a different type of business can cooperate to manage the blockchain network. Furthermore, by utilizing distributed ledger technology, AFOTAK generates an OTAK within a very short period of time (please refer to Appendix I), enabling a faster authentication procedure compared to existing authentication methods, such as public key-based authentication, one-time password, etc.



- 9 -
SG17-C0349

Annex A

A.1 justification for proposed draft new ITU-T X.afotak: "Authentication framework based on One-Time Authentication Key using Distributed Ledger Technology "

Question:	Q10/17	**Proposed new ITU-T Recommendation**	Goyang, 29 August – 8 September, 2023	
Reference and title:	X.afotak: Authentication framework based on One-Time Authentication Key using Distributed Ledger Technology			
Base text:	Annex B of this Contribution		**Timing:**	2025-Aug
Editor(s):	Hyungseung Ko, Korea (Republic of), hsko@fnsvalue.co.kr Seung Ju Jeon, Korea (Republic of), jkme098@fnsvalue.co.kr Heung Youl Youm, Korea (Republic of), hyyoum@sch.ac.kr Sungchae Park, Korea (Republic of), zoesc.park@sch.ac.kr Hun Joo Chang, Korea (Republic of), hannah@fnsvalue.co.kr		**Approval process:**	TAP

Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

This Recommendation provides an authentication framework based on One-Time Authentication Key using Distributed Ledger Technology. It also includes the followings:

- defines the One-time Authentication Key based authentication model and its authentication procedures;
- specifies general requirements and operational protocols for One-time Authentication Key based authentication framework;
- describes how One Time Authentication Key (OTAK) is generated; and
- identifies security threats and specifies security controls.

In addition, it describes service use cases of the One-time Authentication Key based authentication framework as an Appendix, which shows that the proposed authentication framework is applicable to all users, including individual users, organization users, institution users and company users. In addition, it can be applied to super apps' providers, which provide the convenience of accessing multiple services such as payments, messaging, and social media all within one application.

This Recommendation does not address issues related to regulation.

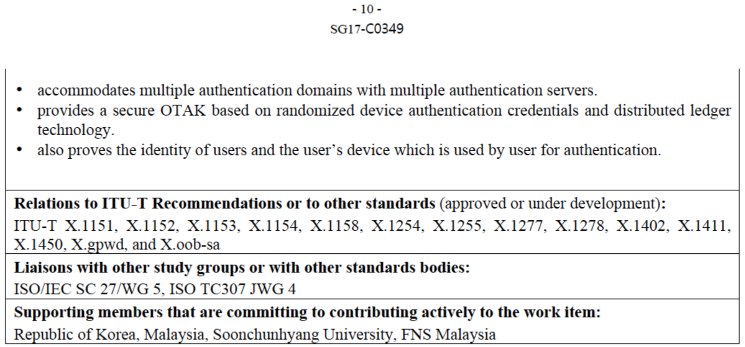
Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

This Recommendation proposes the authentication framework based on One-Time Authentication Key using Distributed Ledger Technology, to expand the scalability of authentication domain and provide one-time authentication key for user authentication. This One-time Authentication Key based authentication framework is based on hybrid blockchain where one entity manages a blockchain network while a group of authentication domains participates in a blockchain network.

The One-time Authentication Key based authentication framework can accommodate multiple authentication domains where a different type of business can cooperate to manage the blockchain network. The One-time Authentication Key based authentication framework is composed of users, service providers, authentication servers which reside on the hybrid blockchain network.

The authentication procedures of AFOTAK consist of two steps: the first step involves verifying the user's device subject to authentication, while the second step involves verifying the user using the OTAK. Regarding the first step, it provides a mechanism to verify the user's device based on distributed ledger technology. Regarding the second step, it provides a mechanism to generate an OTAK by combining randomized device authentication credentials and distributed ledger technology. This OTAK can be a replacement of existing password.

The advantages of this framework are as follows:



- 10 -
SG17-C0349

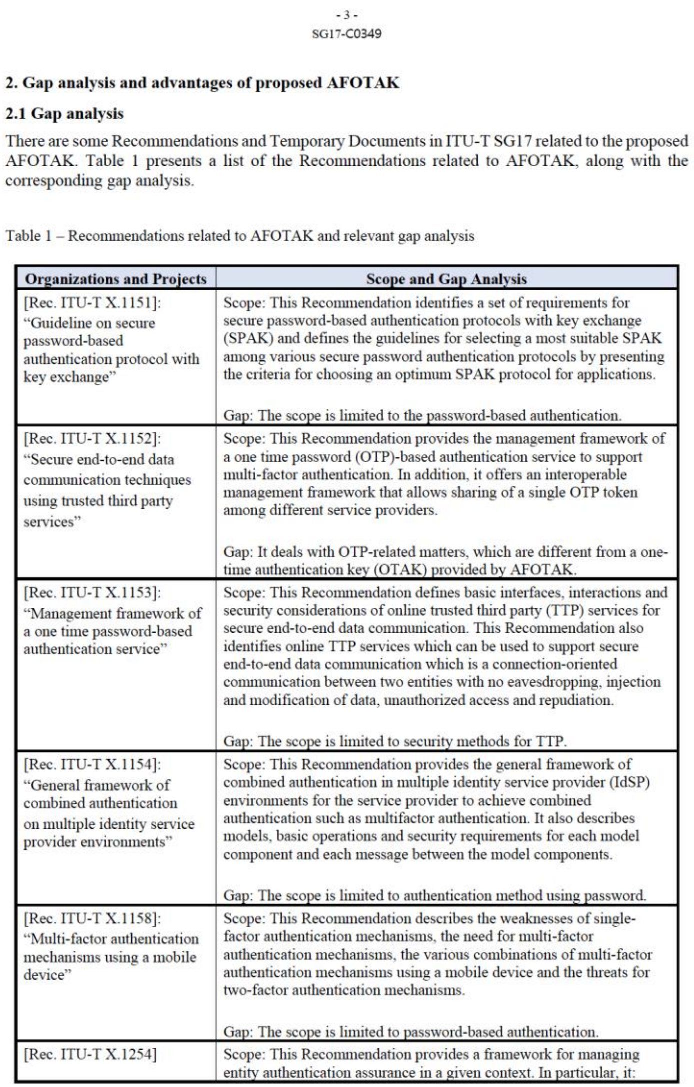
- accommodates multiple authentication domains with multiple authentication servers.
- provides a secure OTAK based on randomized device authentication credentials and distributed ledger technology.
- also proves the identity of users and the user's device which is used by user for authentication.

Relations to ITU-T Recommendations or to other standards (approved or under development):
ITU-T X.1151, X.1152, X.1153, X.1154, X.1158, X.1254, X.1255, X.1277, X.1278, X.1402, X.1411, X.1450, X.gpwd, and X.oob-sa

Liaisons with other study groups or with other standards bodies:
ISO/IEC SC 27/WG 5, ISO TC307 JWG 4

Supporting members that are committing to contributing actively to the work item:
Republic of Korea, Malaysia, Soonchunhyang University, FNS Malaysia

08. 멘토링 주요 내용 및 성과



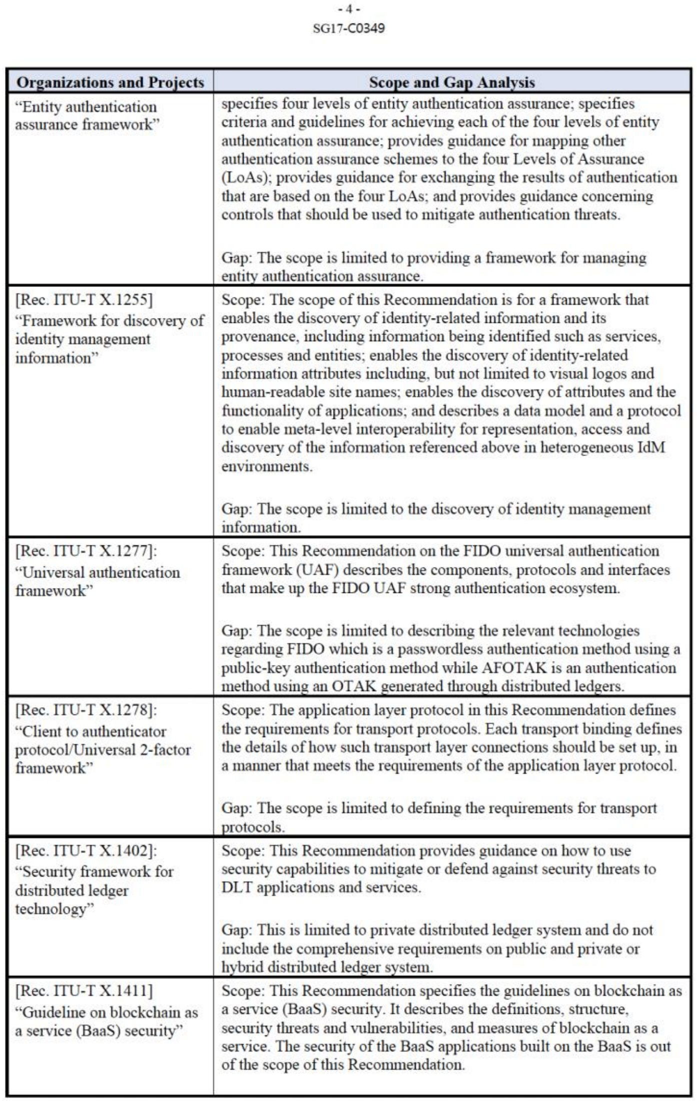
2. Gap analysis and advantages of proposed AFOTAK

2.1 Gap analysis

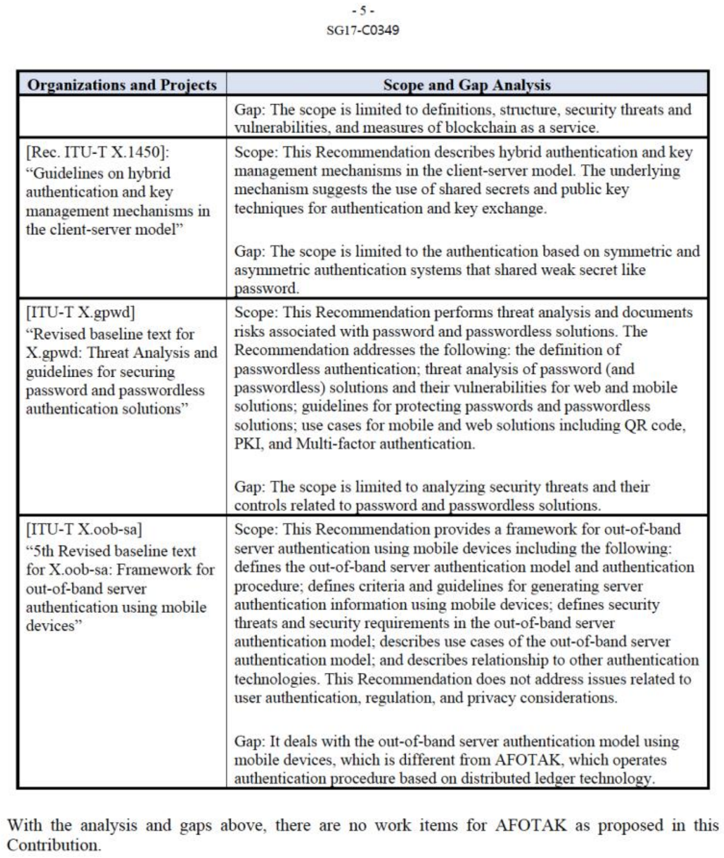
There are some Recommendations and Temporary Documents in ITU-T SG17 related to the proposed AFOTAK. Table 1 presents a list of the Recommendations related to AFOTAK, along with the corresponding gap analysis.

Table 1 – Recommendations related to AFOTAK and relevant gap analysis

Organizations and Projects	Scope and Gap Analysis
[Rec. ITU-T X.1151]: “Guideline on secure password-based authentication protocol with key exchange”	Scope: This Recommendation identifies a set of requirements for secure password-based authentication protocols with key exchange (SPAK) and defines the guidelines for selecting a most suitable SPAK among various secure password authentication protocols by presenting the criteria for choosing an optimum SPAK protocol for applications. Gap: The scope is limited to the password-based authentication.
[Rec. ITU-T X.1152]: “Secure end-to-end data communication techniques using trusted third party services”	Scope: This Recommendation provides the management framework of a one time password (OTP)-based authentication service to support multi-factor authentication. In addition, it offers an interoperable management framework that allows sharing of a single OTP token among different service providers. Gap: It deals with OTP-related matters, which are different from a one-time authentication key (OTAK) provided by AFOTAK.
[Rec. ITU-T X.1153]: “Management framework of a one time password-based authentication service”	Scope: This Recommendation defines basic interfaces, interactions and security considerations of online trusted third party (TTP) services for secure end-to-end data communication. This Recommendation also identifies online TTP services which can be used to support secure end-to-end data communication which is a connection-oriented communication between two entities with no eavesdropping, injection and modification of data, unauthorized access and repudiation. Gap: The scope is limited to security methods for TTP.
[Rec. ITU-T X.1154]: “General framework of combined authentication on multiple identity service provider environments”	Scope: This Recommendation provides the general framework of combined authentication in multiple identity service provider (IdSP) environments for the service provider to achieve combined authentication such as multifactor authentication. It also describes models, basic operations and security requirements for each model component and each message between the model components. Gap: The scope is limited to authentication method using password.
[Rec. ITU-T X.1158]: “Multi-factor authentication mechanisms using a mobile device”	Scope: This Recommendation describes the weaknesses of single-factor authentication mechanisms, the need for multi-factor authentication mechanisms, the various combinations of multi-factor authentication mechanisms using a mobile device and the threats for two-factor authentication mechanisms. Gap: The scope is limited to password-based authentication.
[Rec. ITU-T X.1254]	Scope: This Recommendation provides a framework for managing entity authentication assurance in a given context. In particular, it:



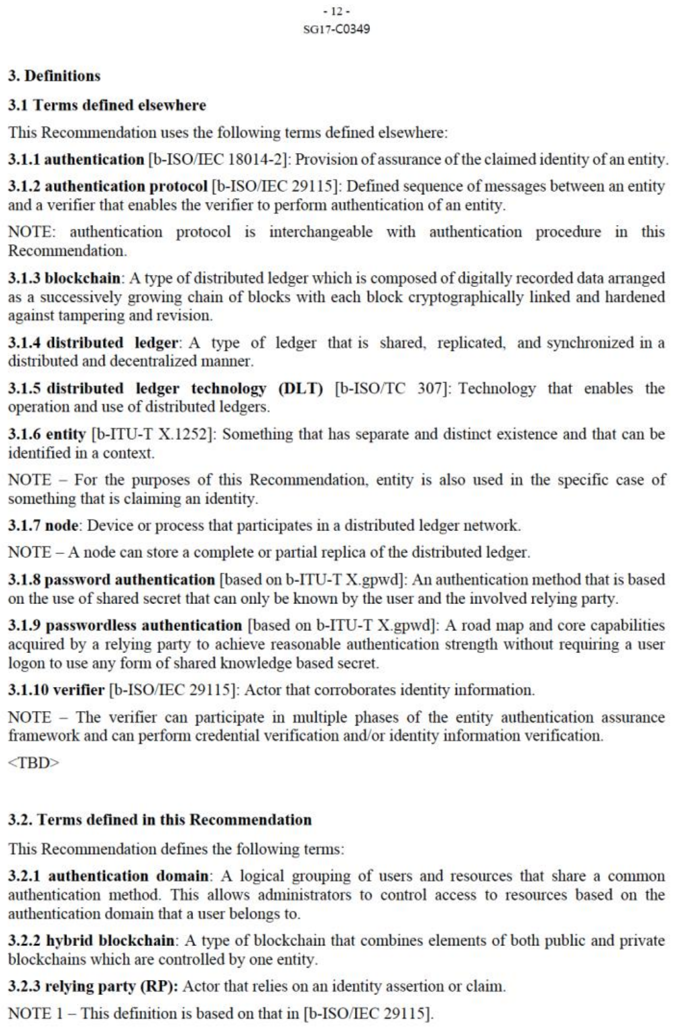
Organizations and Projects	Scope and Gap Analysis
“Entity authentication assurance framework”	specifies four levels of entity authentication assurance; specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance; provides guidance for mapping other authentication assurance schemes to the four Levels of Assurance (LoAs); provides guidance for exchanging the results of authentication that are based on the four LoAs; and provides guidance concerning controls that should be used to mitigate authentication threats. Gap: The scope is limited to providing a framework for managing entity authentication assurance.
[Rec. ITU-T X.1255] “Framework for discovery of identity management information”	Scope: The scope of this Recommendation is for a framework that enables the discovery of identity-related information and its provenance, including information being identified such as services, processes and entities; enables the discovery of identity-related information attributes including, but not limited to visual logos and human-readable site names; enables the discovery of attributes and the functionality of applications; and describes a data model and a protocol to enable meta-level interoperability for representation, access and discovery of the information referenced above in heterogeneous IdM environments. Gap: The scope is limited to the discovery of identity management information.
[Rec. ITU-T X.1277]: “Universal authentication framework”	Scope: This Recommendation on the FIDO universal authentication framework (UAF) describes the components, protocols and interfaces that make up the FIDO UAF strong authentication ecosystem. Gap: The scope is limited to describing the relevant technologies regarding FIDO which is a passwordless authentication method using a public-key authentication method while AFOTAK is an authentication method using an OTAK generated through distributed ledgers.
[Rec. ITU-T X.1278]: “Client to authenticator protocol/Universal 2-factor framework”	Scope: The application layer protocol in this Recommendation defines the requirements for transport protocols. Each transport binding defines the details of how such transport layer connections should be set up, in a manner that meets the requirements of the application layer protocol. Gap: The scope is limited to defining the requirements for transport protocols.
[Rec. ITU-T X.1402]: “Security framework for distributed ledger technology”	Scope: This Recommendation provides guidance on how to use security capabilities to mitigate or defend against security threats to DLT applications and services. Gap: This is limited to private distributed ledger system and do not include the comprehensive requirements on public and private or hybrid distributed ledger system.
[Rec. ITU-T X.1411] “Guideline on blockchain as a service (BaaS) security”	Scope: This Recommendation specifies the guidelines on blockchain as a service (BaaS) security. It describes the definitions, structure, security threats and vulnerabilities, and measures of blockchain as a service. The security of the BaaS applications built on the BaaS is out of the scope of this Recommendation.



Organizations and Projects	Scope and Gap Analysis
	Gap: The scope is limited to definitions, structure, security threats and vulnerabilities, and measures of blockchain as a service.
[Rec. ITU-T X.1450]: “Guidelines on hybrid authentication and key management mechanisms in the client-server model”	Scope: This Recommendation describes hybrid authentication and key management mechanisms in the client-server model. The underlying mechanism suggests the use of shared secrets and public key techniques for authentication and key exchange. Gap: The scope is limited to the authentication based on symmetric and asymmetric authentication systems that shared weak secret like password.
[ITU-T X.gpwd] “Revised baseline text for X.gpwd: Threat Analysis and guidelines for securing password and passwordless authentication solutions”	Scope: This Recommendation performs threat analysis and documents risks associated with password and passwordless solutions. The Recommendation addresses the following: the definition of passwordless authentication; threat analysis of password (and passwordless) solutions and their vulnerabilities for web and mobile solutions; guidelines for protecting passwords and passwordless solutions; use cases for mobile and web solutions including QR code, PKI, and Multi-factor authentication. Gap: The scope is limited to analyzing security threats and their controls related to password and passwordless solutions.
[ITU-T X.oob-sa] “5th Revised baseline text for X.oob-sa: Framework for out-of-band server authentication using mobile devices”	Scope: This Recommendation provides a framework for out-of-band server authentication using mobile devices including the following: defines the out-of-band server authentication model and authentication procedure; defines criteria and guidelines for generating server authentication information using mobile devices; defines security threats and security requirements in the out-of-band server authentication model; describes use cases of the out-of-band server authentication model; and describes relationship to other authentication technologies. This Recommendation does not address issues related to user authentication, regulation, and privacy considerations. Gap: It deals with the out-of-band server authentication model using mobile devices, which is different from AFOTAK, which operates authentication procedure based on distributed ledger technology.

With the analysis and gaps above, there are no work items for AFOTAK as proposed in this Contribution.

08. 멘토링 주요 내용 및 성과



- 12 -
SG17-C0349

3. Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ISO/IEC 18014-2]: Provision of assurance of the claimed identity of an entity.

3.1.2 authentication protocol [b-ISO/IEC 29115]: Defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.

NOTE: authentication protocol is interchangeable with authentication procedure in this Recommendation.

3.1.3 blockchain: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

3.1.4 distributed ledger: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.5 distributed ledger technology (DLT) [b-ISO/TC 307]: Technology that enables the operation and use of distributed ledgers.

3.1.6 entity [b-ITU-T X.1252]: Something that has separate and distinct existence and that can be identified in a context.

NOTE – For the purposes of this Recommendation, entity is also used in the specific case of something that is claiming an identity.

3.1.7 node: Device or process that participates in a distributed ledger network.

NOTE – A node can store a complete or partial replica of the distributed ledger.

3.1.8 password authentication [based on b-ITU-T X.gpwd]: An authentication method that is based on the use of shared secret that can only be known by the user and the involved relying party.

3.1.9 passwordless authentication [based on b-ITU-T X.gpwd]: A road map and core capabilities acquired by a relying party to achieve reasonable authentication strength without requiring a user logon to use any form of shared knowledge based secret.

3.1.10 verifier [b-ISO/IEC 29115]: Actor that corroborates identity information.

NOTE – The verifier can participate in multiple phases of the entity authentication assurance framework and can perform credential verification and/or identity information verification.

<TBD>

3.2. Terms defined in this Recommendation

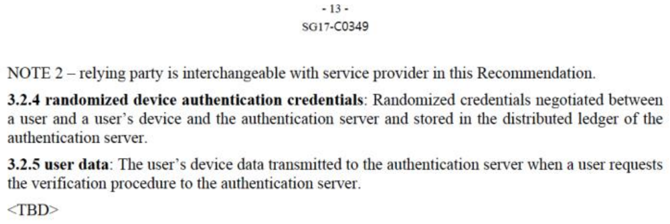
This Recommendation defines the following terms:

3.2.1 authentication domain: A logical grouping of users and resources that share a common authentication method. This allows administrators to control access to resources based on the authentication domain that a user belongs to.

3.2.2 hybrid blockchain: A type of blockchain that combines elements of both public and private blockchains which are controlled by one entity.

3.2.3 relying party (RP): Actor that relies on an identity assertion or claim.

NOTE 1 – This definition is based on that in [b-ISO/IEC 29115].



- 13 -
SG17-C0349

NOTE 2 – relying party is interchangeable with service provider in this Recommendation.

3.2.4 randomized device authentication credentials: Randomized credentials negotiated between a user and a user's device and the authentication server and stored in the distributed ledger of the authentication server.

3.2.5 user data: The user's device data transmitted to the authentication server when a user requests the verification procedure to the authentication server.

<TBD>

11. 멘토링 주요 내용 및 성과

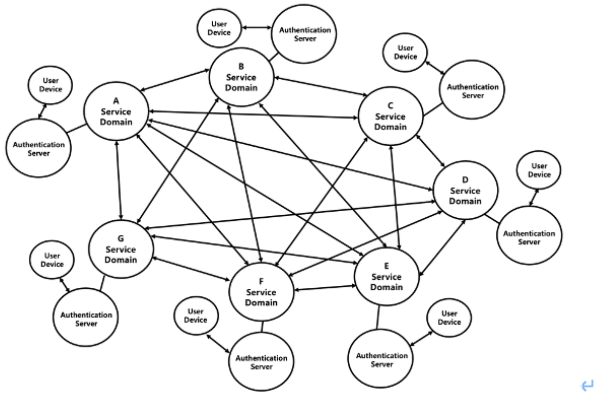


Figure 2 - Sample AFOTAK Network↵

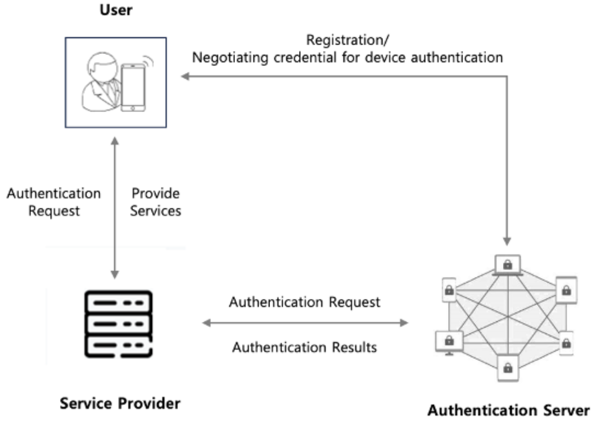


Figure 4 – Entities↵

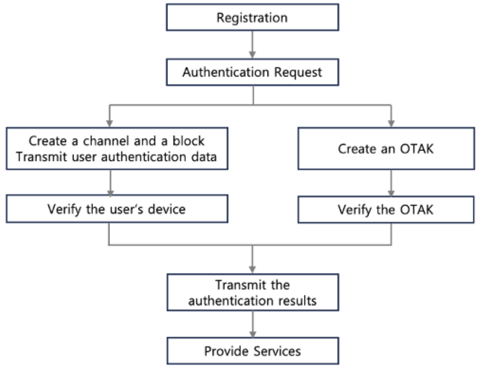


Figure 5 – General Procedures of AFOTAK↵

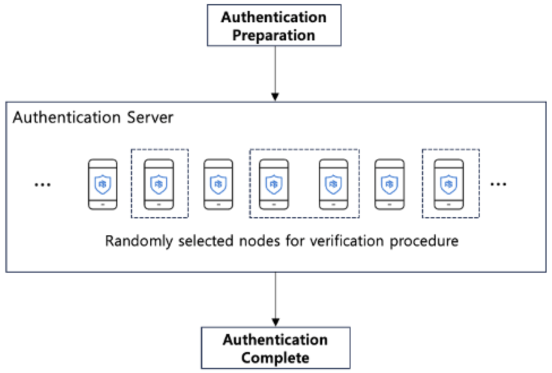

Authentication Preparation
Authentication Server
...
...
Randomly selected nodes for verification procedure
Authentication Complete

Figure 6 – Method for Selecting Nodes↵

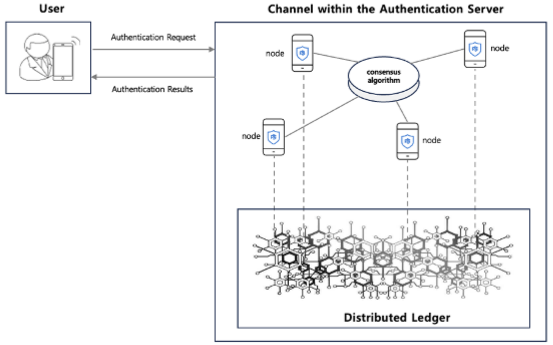


Figure 7 – Method for Verifying User Data↵

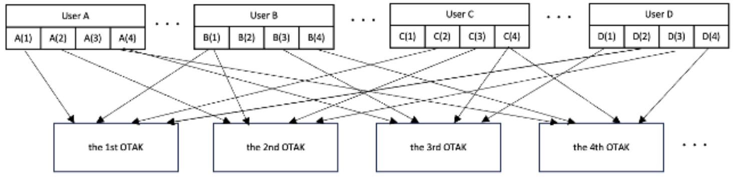
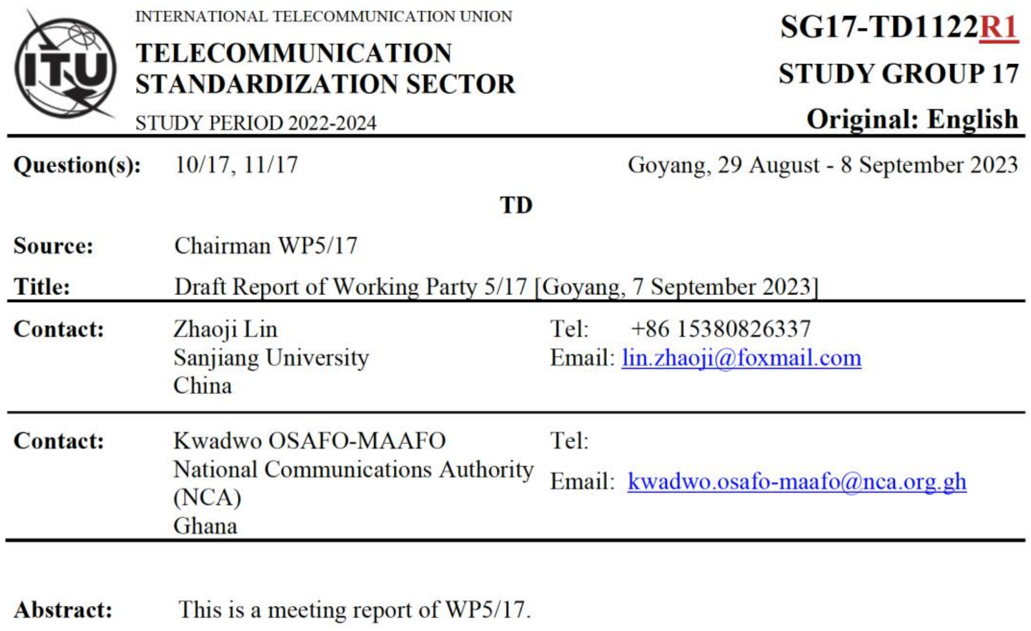


Figure 8 – OTAK Creation Method↵

12. 멘토링 주요 내용 및 성과

- 기고서 및 회의 준비 사항 지원
- Q 10 회의 발표 및 대응 준비 지원
- ITU-T Study Group 17 회의 중 현장 지원
- Interim 회의 등 후속 회의 지원
- ICT 국제 표준화 전문가 및 신진 전문가 안내

13. 멘토링 주요 내용 및 성과



INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2022-2024

SG17-TD1122R1
STUDY GROUP 17
Original: English

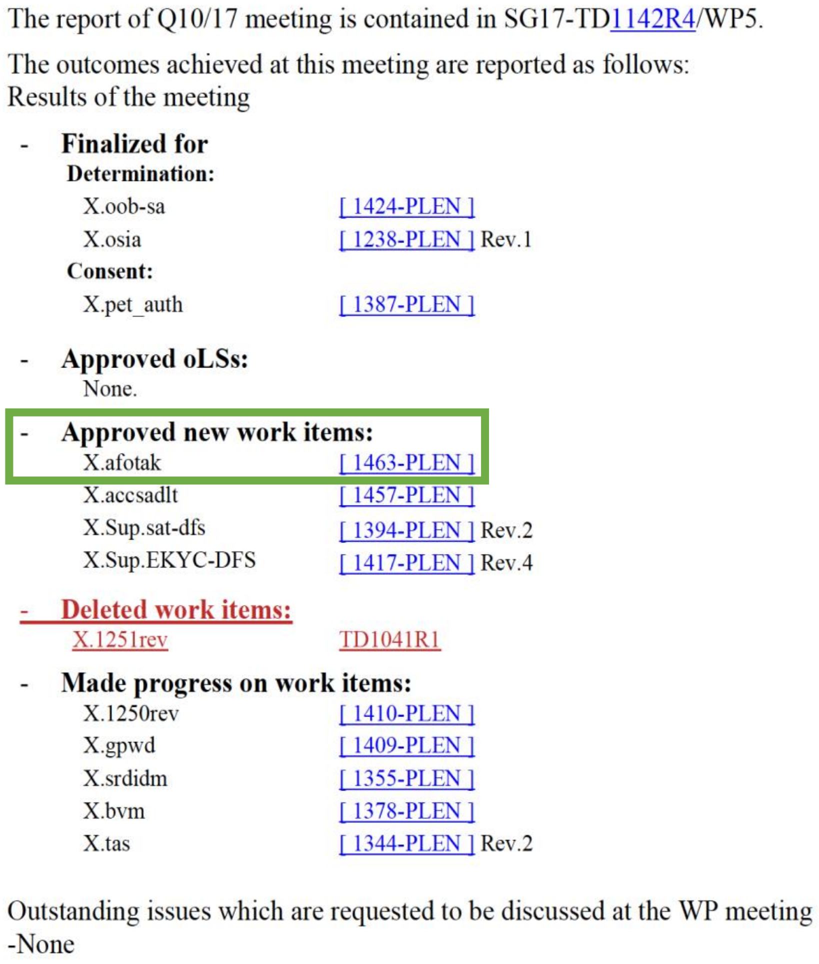
Question(s):	10/17, 11/17	Goyang, 29 August - 8 September 2023

TD

Source:	Chairman WP5/17
Title:	Draft Report of Working Party 5/17 [Goyang, 7 September 2023]

Contact:	Zhaoji Lin Sanjiang University China	Tel: +86 15380826337 Email: lin.zhaoji@foxmail.com
Contact:	Kwadwo OSAFO-MAAFO National Communications Authority (NCA) Ghana	Tel: Email: kwadwo.osafo-maafo@nca.org.gh

Abstract: This is a meeting report of WP5/17.



The report of Q10/17 meeting is contained in SG17-TD1142R4/WP5.

The outcomes achieved at this meeting are reported as follows:
Results of the meeting

- **Finalized for**

Determination:

X.oob-sa	[1424-PLEN]
X.osia	[1238-PLEN] Rev.1

Consent:

X.pet_auth	[1387-PLEN]

- **Approved oLSs:**

None.

- **Approved new work items:**

X.afotak	[1463-PLEN]
X.accsadlt	[1457-PLEN]
X.Sup.sat-dfs	[1394-PLEN] Rev.2
X.Sup.EKYC-DFS	[1417-PLEN] Rev.4

- **Deleted work items:**

X.1251rev	TD1041R1

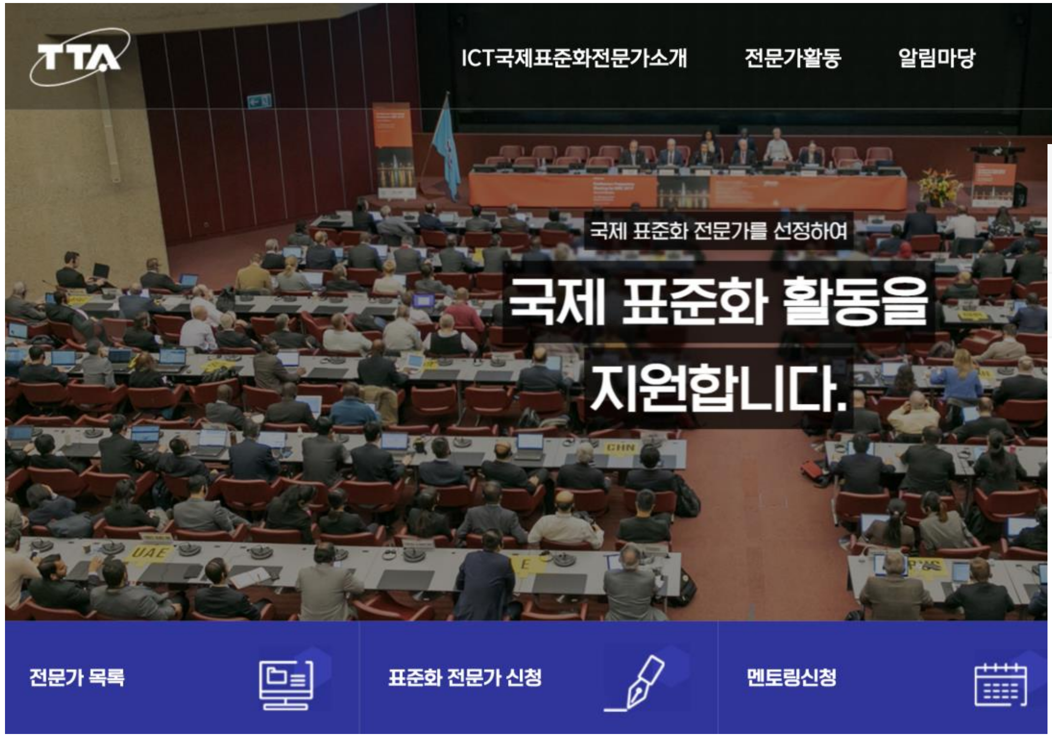
- **Made progress on work items:**

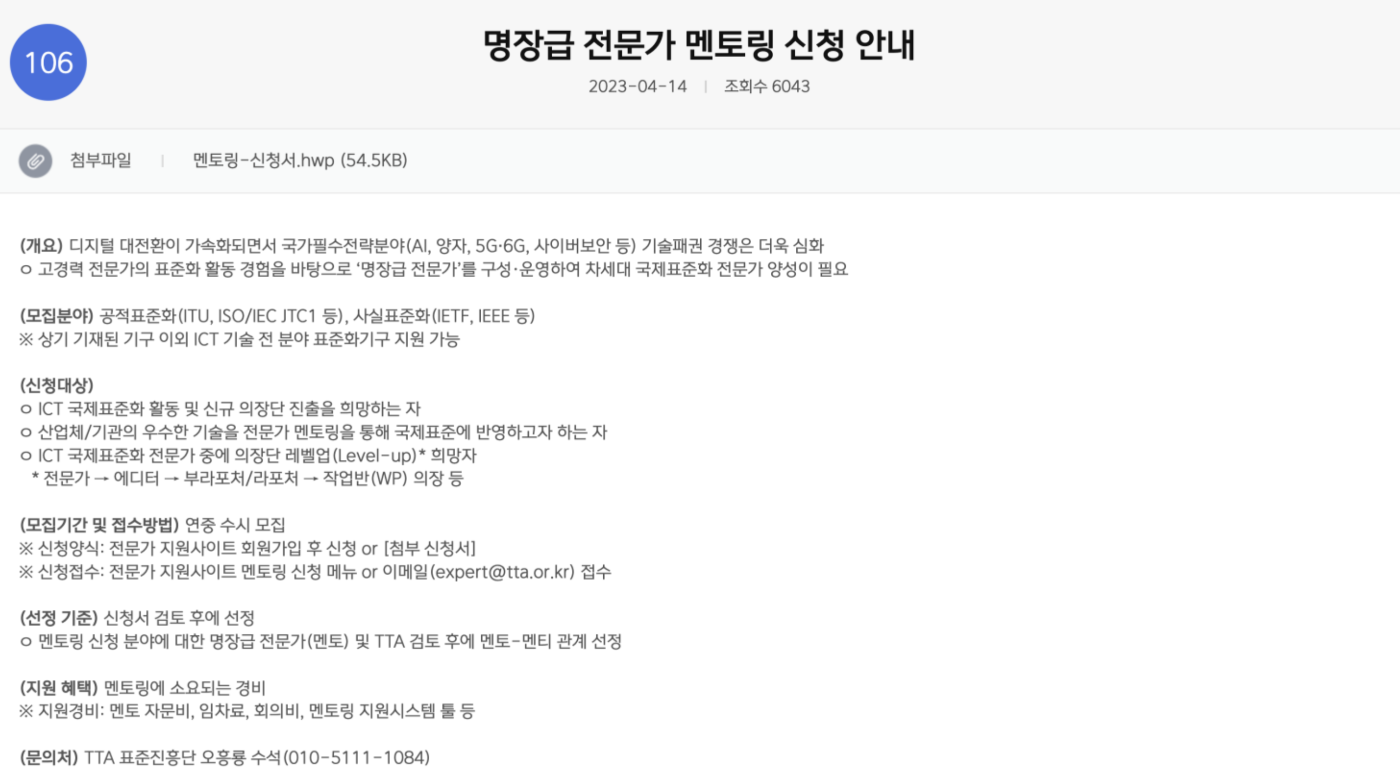
X.1250rev	[1410-PLEN]
X.gpwd	[1409-PLEN]
X.srdidm	[1355-PLEN]
X.bvm	[1378-PLEN]
X.tas	[1344-PLEN] Rev.2

Outstanding issues which are requested to be discussed at the WP meeting
-None

14. 멘토링 주요 내용 및 성과

한국 정보통신 기술 협회: https://expert.tta.or.kr





106

명장급 전문가 멘토링 신청 안내

2023-04-14 | 조회수 6043

첨부파일 | 멘토링-신청서.hwp (54.5KB)

(개요) 디지털 대전환이 가속화되면서 국가필수전략분야(AI, 양자, 5G·6G, 사이버보안 등) 기술패권 경쟁은 더욱 심화
○ 고경력 전문가의 표준화 활동 경험을 바탕으로 '명장급 전문가'를 구성·운영하여 차세대 국제표준화 전문가 양성이 필요

(모집분야) 공적표준화(ITU, ISO/IEC JTC1 등), 사실표준화(IETF, IEEE 등)
※ 상기 기재된 기구 이외 ICT 기술 전 분야 표준화기구 지원 가능

(신청대상)
○ ICT 국제표준화 활동 및 신규 의장단 진출을 희망하는 자
○ 산업체/기관의 우수한 기술을 전문가 멘토링을 통해 국제표준에 반영하고자 하는 자
○ ICT 국제표준화 전문가 중에 의장단 레벨업(Level-up)* 희망자
* 전문가 → 에디터 → 부라포처/라포처 → 작업반(WP) 의장 등

(모집기간 및 접수방법) 연중 수시 모집
※ 신청양식: 전문가 지원사이트 회원가입 후 신청 or [첨부 신청서]
※ 신청접수: 전문가 지원사이트 멘토링 신청 메뉴 or 이메일(expert@tta.or.kr) 접수

(선정 기준) 신청서 검토 후에 선정
○ 멘토링 신청 분야에 대한 명장급 전문가(멘토) 및 TTA 검토 후에 멘토-멘티 관계 선정

(지원 혜택) 멘토링에 소요되는 경비
※ 지원경비: 멘토 자문비, 임차료, 회의비, 멘토링 지원시스템 툴 등

(문의처) TTA 표준진흥단 오흥룡 수석(010-5111-1084)

GISC
2023

Global ICT Standards Conference 2023

감사합니다.

고형승 미국변호사(팀장), (주)에프엔에스벨류
hsko@fnsvalue.co.kr