|  |  |  |
| --- | --- | --- |
|  | World Telecommunication Standardization Assembly (WTSA-24)New Delhi, 15–24 October 2024 |  |
|  |
|  |  |
| PLENARY MEETING | Addendum 40 toDocument 37-E |
|  | 22 September 2024 |
|  | Original: English |
|  |
| Asia-Pacific Telecommunity Member Administrations |
| DRAFT NEW RESOLUTION [APT-DI] - PROMOTING STANDARDIZATION WORK FOR DIGITAL IDENTITIES AND CREDENTIALS |
|  |
|  |

|  |  |
| --- | --- |
| **Abstract:** | This document contains the proposal for new WTSA resolution on promoting standardization work for digital identities and credentials. |
| **Contact:** | Mr. Masanori Kondo Secretary GeneralAsia-Pacific Telecommunity | E-mail: aptwtsa@apt.int  |

Introduction

A digital identity is typically defined as a one-to-one relationship between an individual and their digital presence. A digital presence can consist of multiple accounts, credentials, and entitlements associated with an individual. Identity Management includes issuing, validating (proofing), maintaining, and terminating identities while credentials are pieces of evidence that confirm an individual's claimed identity. For example, a driver's license or an online ID and password tie the credential owner to his or her identity.

Decentralized identity is a new paradigm where it allows users to manage and share their identity data without relying on a central authority or third-party service.

Digital identity and verifiable credential need to support efforts to enhance online security for underage individuals by proving identity attributes, such as age verification and enforcement.

Verifiable credentials are digital documents that are cryptographically secure and can be used to prove various aspects of a user's identity without exposing unnecessary personal information. Examples of verifiable credentials include digital employee cards, digital birth certificates, mobile driver's licenses, and digital education certificates, digital national number certificates, biometric data certificates.

Digital identity, including verifiable credentials, is considered a personal identification tool used to access online services, make purchases, and interact with others on digital platforms.

Fraudulent identities and credentials could be created using AI/ML algorithms that can generate realistic-looking digital identities and credentials in a matter of minutes.

ITU-T SGs, particularly SG17, need to advance work on digital identity standardization in order to build security and confidence in the use of ICTs. SG17 is the lead study group on identity management, which includes work for digital identity and credential. We believe that this new resolution will facilitate digital transformation and help developing countries to bridge the standardization gap.

ITU-T has a role to play in developing technical standards in the areas of digital identity and verifiable credentials, which are key enabling technologies to provide innovation of ICT services and applications.

Proposal

Based on the background above, APT Member Administrations propose to WTSA-24 to consider establishment of anew WTSA resolution on promoting standardization work for digital identities and credentials.

ADD APT/37A40/1

DRAFT NEW RESOLUTION [APT-DI] (New Delhi, 2024)

Promoting standardization work for digital identities and credentials

(New Delhi, 2024)

The World Telecommunication Standardization Assembly (New Delhi, 2024)

recalling

*a)* Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, on strengthening the role of ITU in building confidence and security in the use of information and communication technologies (ICTs);

*b)* Resolution 179 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, on ITU's role in child online protection;

*c)* Resolution 50 (Rev. Geneva, 2022) of the World Telecommunication Standardization Assembly (WTSA), on cybersecurity*,*

considering

*a)* the importance of digital identities as tools for identifying an individual, which are used to access online services, make purchases, and interact with other individuals and systems on digital platforms;

*b)* the importance of verifiable credentials, such as digital documents, as tools for confirming an individual's claimed identity;

*c)* the fundamental role of digital identities and verifiable credentials, in the use of information and communication technologies (ICTs) such as artificial intelligence, distributed ledger technologies, digital twins, metaverse technologies and Internet of Things;

*d)* the ubiquitous mobile device such as a smartphone or tablet is an increasingly popular tool for proving that we are who we claim to be (the process known as authentication) in everyday digital transactions;

*e)* the need for globally interoperable digital identities and verifiable credentials, properly de-duplicated with the inherent biometric properties of individuals;

*f)* digital identities and verifiable credentials are equipped with security, like better control over online data, scalability, and flexibility over paper-based identities;

*g)* identity wallets allow people to store digital identity and verifiable credentials, such as ID cards, driver’s licenses, and social security details, all in one place on mobile devices;

*h)* interoperable digital identities enable people to use their verifiable credentials for facilitating various online services across borders, such as accessing medical records, financial services, tax returns, online money transfers, and other government sites;

*i)* decentralized identity is a digital identity management system where individuals have complete control over their identity data and it allows users to manage and share their identity data without relying on a central authority or third-party service;

*j)* decentralized identity concepts such as verifiable credentials can be used to verify identity attestation about age, residence, and location;

*k)* biometric data as a kind of digital identity facilitates and promotes digital identity management;

*l)* privacy-enhancing technologies such as zero knowledge proofing technology can be used to ensure the trustworthiness of digital identity and verifiable credentials;

*m)* the importance of decentralized identity for ensuring accountability and traceability;

*n)* the use of AI/ML in the domain of digital identity such as liveness detection, face recognition, combating bias, etc., and to enhance digital identity and security

*o)* that ITU-T has a role to play, within its mandate and competencies, in regard to digital identity and verifiable credentials including decentralized identity,

considering further

*a)* that the joint coordination activity on identity management under the auspices of ITU‑T SG17 coordinates works in the area of identity management across the ITU-T study groups and other relevant groups;

*b)* that Recommendation ITU‑T X.1254 specifies three entity authentication assurance levels (AALs), and criteria for and threats to each of them;

*c)* that Recommendation ITU-T X.1277.2 provides authentication without passwords by using biometrics and other modalities to authenticate users to their local device. Additionally, Recommendation ITU-T X.1278.2 allows the use of external authenticators for authentication and describes an application layer protocol for communication between a roaming authenticator and another client/platform, as well as bindings of this application protocol to a variety of transport protocols using different physical media;

*d)* that Recommendation ITU-T X.1403 provides an overview of using distributed ledger technology for decentralized identity management;

*e)* that ITU‑T and the Joint Technical Committee for information technology (JTC 1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), as well as several consortia and standards entities such as the World Wide Web consortium (W3C), the Organization for Advancement of Structured Information Standards (OASIS), the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE), among others, already have a significant body of published materials and ongoing work that is directly relevant to this topic, which needs to be considered,

noting

*a)* that ITU-T Study Group 17 is the lead study group on identity management, assigned with the task of coordinating identity management activities within ITU‑T and with other standards‑development organizations and forums, and developing frameworks to improve collaboration;

*b)* that a wide range of bodies and organizations are working on digital identity and verifiable credentials standards,

recognizing

*a)* the relevant achievements of ITU‑T Study Group 17 in the areas of identity management and telebiometrics architecture and mechanisms, such as security guidelines for using distributed ledger technology for decentralized identity management specified in Recommendation ITU-T X.1403;

b) there is clear need for coordinating work among ITU-T study groups and other standards development organizations,

resolves

1 to continue to develop the necessary Recommendations, Supplements, technical reports on digital identities and verifiable credentials;

2 to continue to develop best practices for establishing interoperable, trustworthy digital identities and verifiable credentials to be used by telecommunication/ICT infrastructure providers;

3 to promote standardization work for digital identities and verifiable credentials including decentralized identities;

4 that ITU‑T should work concerning digital identities and verifiable credentials with ITU‑D, particularly in the context of ITU-D Question 3/2 (Securing information and communication networks: best practices for developing a culture of cybersecurity),

instructs Study Group 17 of the ITU Telecommunication Standardization Sector with the support of other study groups

1 to evaluate existing and evolving ITU-T Recommendations, ITU-T publications including standards or specifications by other SDOs and, based on the assessment, to develop new Recommendations, best practices and other ITU-T publications with respect to digital identities and verifiable credentials;

2 to promote joint coordination activity with other study groups and other standardization organisations with a view to a harmonized approach of establishing global, interoperable digital identities and verifiable credentials;

3 to support the Director of TSB to maintain the Identity management Standards Roadmap, which should include work items to progress standardization work related to identity management, and share those with relevant groups of the ITU Radiocommunication Sector (ITU-R) and ITU-D as the mission of the lead study group for identity management;

4 to continue to provide regular reports on identity management including digital identities and verifiable credentials to the Telecommunication Standardization Advisory Group, including on how to address the topics that are outside the mandate of the study groups,

instructs the Telecommunication Standardization Advisory Group

to drive a concerted effort across relevant study groups to accelerate standardization work on digital identities and verifiable credentials including decentralized identity;

instructs the Director of the Telecommunication Standardization Bureau

1 to create, with the assistance of other relevant organizations, an inventory of national, regional and international initiatives and activities to promote, to the extent possible, the worldwide harmonization of strategies and approaches in this critically important area, including the development of common approaches in the field of digital identities and verifiable credentials;

2 to continue to cooperate with the Director of the Telecommunication Development Bureau to facilitate the promoting of use of digital identities and verifiable and trustworthy credentials and in the implementation of this resolution, and to develop guidance on the digital identities and verifiable credential to build security and confidence in the use of ICTs,

invites Member States, Sector Members, Associates and Academia

1 to provide information on national, regional and international initiatives and activities;

2 to submit contributions developing Recommendations and best practices for digital identities.