Question 10/17 – Management of digital identity

(Continuation of Question 10/17 (2024)[*])

1 Motivation

Identity management (IdM) governs the life cycle of credentials, identifiers, attributes, and patterns, managing their creation, maintenance, utilization, and revocation. It enables service providers, end-users, organizations, network devices, applications, and services to establish mutual trust. A single entity may use multiple identities with different security requirements across various locations. Organizations can implement IdM in centralized, decentralized, or hybrid models, depending on the identity framework. "Digital identity serves as the foundation for implementing IdM. It defines 'what' the identity is, while IdM focuses on 'how' that identity is managed within the digital ecosystem. Decentralized Identity (DID) represents a paradigm shift in digital identity management, offering improved tools and methods for enhancing online identity management."

A digital identity wallet is a secure tool for storing, managing, and sharing digital identity information, such as verifiable credentials, and decentralized IDs with others. It gives users full control over their personal data and its use.

In public networks, IdM enables authorized entities to exchange trusted information by asserting identities across distributed systems from multiple service providers. This applies to service environments such as cloud, IMT-2020, and IMT-2030. IdM also enhances privacy by restricting access to protected information based on a predefined trust model.

The increasingly widespread access to telecommunications/ICTs worldwide, in particular the Internet, and use thereof by unauthorized actors (e.g. minors) necessitates the development of technical standards to support efforts to enforce access policies.

The increasingly widespread access to agentic AI acting in lieu of entities require the development of standards based on AI entities as a part of digital identity management.

In telecommunications and ICT networks, IdM plays a critical role in authentication and access control. It grants or restricts access based on privileges and updates permissions when an entity’s role changes. IdM also supports delegation, and other identity-based services, ensuring secure and flexible identity management.

From a security perspective, IdM strengthens network protection by enabling secure, on-demand access to networks and services, particularly for mobile users. It helps prevent fraud and identity theft, reinforcing user confidence in secure transactions. Since IdM operates on mutual trust, both end users and service providers benefit from its safeguards.

As IdM specifications and solutions evolve, establishing a foundation for interoperability remains essential. This Question defines a strategic vision and coordinates IdM activities within ITU-T while ensuring collaboration with other study groups and standards development organizations (SDOs). While some ITU-T Questions focus on specific aspects of IdM such as protocols, requirements, and network device identifiers, this initiative provides overall direction and alignment.

With expanding cross-border movement and global supply chains, communication and data exchange increasingly occur in cyberspace, spanning multiple countries and organizations. Effective collaboration relies on interoperability across digital IDs, trust services, management systems, standardized operational processes and common frameworks to ensure smooth and secure cooperation.

---

[*] Update of Q10/17 "*Telecommunication information security management and security services*" (WTSA-24) as prepared by ITU-T SG17 (Geneva, 8-17 April 2025) and endorsed by TSAG (Geneva, 26-30 May 2025).

Biometrics plays a growing role in identity verification for applications such as e-commerce, telemedicine, and e-health. However, biometric systems must address operational and technical challenges related to data protection, reliability, and security, particularly in biosafety and biosecurity applications. Biometrics can be utilized to enhance reliability, and security of authentication for identity verification.

Deploying biometric authentication in open networks raises security concerns. Telecommunication applications, including telebiometrics for mobile and Internet-based services, require authentication methods that balance strong security with user convenience. Clear requirements ensure that telebiometric data is handled safely, securely and with robust operational and data protection.

Recommendations and Supplements under responsibility of this Question as of 12 September 2024: X.1080.0, X.1080.1, X.1080.2, X.1081, X.1082, X.1083, X.1084, X.1085, X.1086, X.1087, X.1088, X.1089, X.1090, X.1091, X.1092, X.1093, X.1094, X.1095, X.1250, X.1251, X.1252, X.1253, X.1254, X.1255, X.1256, X.1257, X.1258, X.1261 (with SG2), X.1275, X.1276, X.1277, X.1278, X.1279, X.1280, X.1281, X.1283,and Supplements 7, 35, 41, and 42.

Texts under development as of 12 September 2024: X.1282 (X.afotak), X.1250rev, X.1254rev, X.accsadlt, X.bvm, X.oicc, X.oob-pacs, X.srdidm, X.tas, X.tis, X.vctp, and Technical Reports TR.divs, TR.SIMRegBio.

2 Question

Study items to be considered include, but are not limited to:

- What are the essential functional concepts, components, and architectural considerations for a user-centric, cloud-compatible, and decentralized identity management (IdM) framework that ensures security, privacy, consent, and interoperability across different systems, while supporting technologies such as identity wallets, decentralized identifiers (DIDs), and verifiable credentials?
- What are the requirements, capabilities, and possible strategies for achieving interoperability between different IdM systems (e.g., identity assurance, inter-working)?
- What are the key considerations for supporting identity on distributed ledger technologies, including digital identity wallets, decentralized identifiers, and verifiable credentials?
- What are the requirements and mechanisms for protecting and disclosing personally identifiable information (PII)?
- How can an entity control its relationship when involved in identity-based relationships and interactions?
- How can integrating Identity IdM systems with advanced security technologies enhance their ability to prevent and respond to threats effectively?
- How PKI based authentication be performed in an interoperable and secure manner?
- What are the unique requirements for consumer-based identity management system in terms of identity vetting and account recovery without reliance on passwords?
- How trust and relationship can be used to enhance account recovery, users' security and experience when dealing with relying parties?
- How standardization efforts can be better supported for enhancing security online for underage individuals, identity attribute attestations such as age verification and enforcement?
- How can trusted registries be used to enable accountable Identity and Access Management (IAM) directories, and what specifications need to be developed?
- How can decentralized identity concepts, such as verifiable credentials, be used to verify identity attributes like age, residence, and location?

- How can identity management systems deliver identity management as a service to support cloud agents, IMT-2020, IMT-2030 networks, and mobile devices, ensuring scalability, security, and interoperability across these environments?
- What is the impact of AI on biometrics and identity management?
- What are the specific IdM requirements of service providers?
- What mechanisms need to be supported to ensure safe and secure manipulation of biometric data in not only existing but also emerging applications of telebiometrics, e.g., e-health, tele-medicine, video surveillance?
- What are the requirements and capabilities of IdM systems to protect against cyber-attacks?
- What are the candidate mechanisms for identity management (IdM) interoperability, including the identification and definition of applicable profiles to minimize interoperability challenges?
- How can trusted identity management systems support federation across systems, services, devices, IoT, and applications?
- What are the similarities and differences between the existing biometrics Recommendations in ITU-T and the standards in ISO/IEC?
- What are the key requirements for ID management systems and trust mechanism to function in an integrated manner, and what essential functions and components are needed to achieve this?
- What type of system should support an organization's security posture in the current cyber landscape, and what essential governance functions should it incorporate for security strategy and its related operational management?
- What requirements should ID management systems and trust mechanism fulfill within a system that supports an organization's security posture?
- What are the requirements and mechanisms for identity assurance in authentication and federation, and how can different identity assurance methods be mapped and interworked across various networks?
- How biometrics be used as part of a strong authentication and trust layer to enable trusted interactions over a network?
- What are the requirements for evaluating security, operational, and technical data protection techniques in the application of biometrics?
- What are the requirements for integrating biometric authentication into a trusted identity framework?
- What are the requirements for biometric authentication in an advanced, high-performance, and secure network?
- How can the effectiveness of security measures for protecting biometric systems be assessed concerning the specific risks and requirements of their intended applications?
- How should biometric systems and operations be developed in order to be conformant to the security requirements for any application of biometrics, including cloud computing services?
- How can identification and authentication of users be improved in the aspects of safety and security by the use of interoperable models in biometrics?
- How can biological metrics be transmitted between biological systems and machines, and how can they interoperate with existing machine-to-machine protocols?
- How can bio-signals be utilized for telebiometric applications, and what are some potential uses for them?

– What frameworks enable global interoperability for a digital identity wallet within a decentralized identity eco-system?
– What are the digital identity requirements to enforce access policies based on user preferences?
– What are the requirements to extend digital identity management to support management of agentic AI entities.

3 Tasks

Tasks include, but are not limited to:

– Study, analyse, and design a comprehensive identity management (IdM) framework that prioritizes user control, cloud compatibility, and decentralized technologies such as blockchain, digital identity wallets, decentralized identifiers (DIDs), and verifiable credentials. Ensure interoperability, security, privacy, and explicit user consent by defining essential functional concepts, key components, and architectural considerations, while addressing scalability, trust models, and governance mechanisms for secure identity exchange.
– Identify key requirements and security standards, analyse the capabilities of existing IdM systems, develop interoperability models and strategies for cross-platform communication, test solutions for security and functionality, and establish governance and policy frameworks for seamless identity exchange and verification.
– Study the technical, security, privacy, and interoperability challenges of integrating digital identity wallets, decentralized identifiers, and verifiable credentials with distributed ledger technologies. Develop decentralized identity management systems that prioritize user control over their identities, ensuring data privacy and compliance with relevant security standards.
– Identify the requirements (e.g., regulatory), technical mechanisms (e.g., encryption, access control), and disclosure mechanisms (e.g., transparency, third-party contracts) to protect and disclose PII in the context of IdM
– Specify an IdM framework that supports discovery, policy and trust model, authentication and authorization, assertions, and credential lifecycle management required for IdM.
– To strengthen authentication, monitor user behaviour, and ensure continuous verification, study how to integrate IdM with advanced security technologies such as MFA, Zero Trust, AI/ML for threat detection, encryption, and DLT for identity verification.
– Analyse PKI standards and protocols (e.g., X.509, TLS, S/MIME), assess cross-certification and PKI federation, evaluate security risks and mitigation strategies (e.g., HSMs, MFA, revocation mechanisms), and benchmark performance and scalability.
– Study and evaluate identity verification technologies, user experience, privacy compliance, consumer trust, scalability, and interoperability to enhance passwordless IdM systems.
– Study and develop mechanisms integrate trusted networks into IdM systems so that account recovery and security become both robust and user-friendly.
– Study and develop robust and secure age verification and online protection methods that incorporate strong privacy protections for underage individuals.
– Study and develop specification for trusted registries as a mean of accountable Identity and Access Management (IAM) directories.
– Use decentralized identity concept such as verifiable credentials to verify identity attestation about age, residence, and location.
– Support identity management system providing identity management as a service for cloud agents, IMT-2020, IMT-2030 networks and mobile devices.

- Identify and assess the impact of AI on biometrics and identity management by identifying benefits, risks, and mitigation strategies, with a focus on practical applications and policy considerations.
- Define requirements and propose mechanisms to protect IdM systems, including strategies for leveraging IdM capabilities to enable service providers to coordinate and exchange information on cyber-attacks.
- Study and develop requirements for generic protocols that ensure safety, security, data protection, and user consent in the handling of biometric data across telebiometrics applications, such as e-health, telemedicine, and video surveillance.
- Define functional IdM architectural concepts to include IdM bridging between networks and among IdM systems, taking into account advanced security technologies.
- Review existing frameworks (e.g., OAuth, OpenID, SAML), evaluate federated, decentralized, and hybrid models, assess the consistency of best practices from W3C, ISO, and FIDO, examine security, privacy, and regulatory compliance, and benchmark IdM mechanisms for scalability, efficiency, and cross-platform compatibility.
- Support of trusted identity management systems that can federate across systems, services, devices, IoT and applications.
- Review the similarities and differences among the existing biometrics Recommendations in ITU-T and standards in ISO/IEC
- Specify requirements for identity management (IdM) systems and trust mechanismto function in an integrated manner, ensuring interoperability, security, privacy, user control, scalability, trust mechanisms, and regulatory compliance. Consider essential functions and components such as authentication, authorization, identity federation, trust anchors, verifiable credentials, policy enforcement, monitoring, and integration through APIs and decentralized technologies.
- Study the design of a comprehensive identity management system that relates to a Cyber Defence Centre (CDC) or Cyber Security Centre (CSC).
- Study the requirements for identity management (IdM) systems, trust mechanism, and CDC/CSC to strengthen an organization's security posture, focusing on IdM functions like authentication, authorization, and access control; trust mechanism needs such as decentralized identifiers (DIDs) and verifiable credentials.
- Specify requirements and propose mechanisms for identity assurance for authentication and federation. Establish criteria for mapping/interworking among different identity assurance methods that might be adopted in various networks. In this context, identity assurance includes identity patterns and reputation.
- Study and define IdM system protection (identify security risks and threats) and develop IdM robust functionalities (secure identity protocols, educate users and align with industry standards).
- Study and develop requirements for evaluating security and operational and technical data protection techniques for any application of biometrics.
- Study and develop requirements of biometric authentication for trust identity framework.
- Study and develop requirements for biometric authentication in advanced, high-performance, and secure networks.
- Assess the effectiveness of security measures for biometric systems, by evaluating potential risks, testing countermeasures against threats, and ensuring they meet the needs of the specific application's security and operational needs.
- Study and develop comprehensive frameworks and requirements for biometric applications in cloud computing and data storage environments.

– Study and develop user identification and authentication systems that enhance security and safety by leveraging decentralized models based on verifiable credentials and centralized models using interoperable biometric frameworks.
– Study and develop biology-to-machine (B2M) protocols for transmitting biological metrics of which interoperate with machine-to-machine (M2M) protocols.
– Study and develop telebiometric applications using bio-signals for applications including but not limited to authentication, identification, and health information monitoring.
– Study and develop a framework for digital identity wallet interoperability based on decentralized identity mechanisms.
– Study and develop digital identity requirements to enforce access policies based on user preferences?
– Study and develop requirements to extend digital identity management to support management of agentic AI entities.

An up-to-date status of work under this Question is contained in the SG17 work programme at https://www.itu.int/ITU-T/workprog/wp_search.aspx?sp=18&q=10/17.

4 Relationships

Recommendations:

– X- and Y-series
– X.200, X.273, X.274, X.509, X.680, X.805 and X.1051

Questions:

– All ITU-T SG17 Questions

Study groups:

– ITU-T SG 2
– ITU-T SG 5
– ITU-T SG 11
– ITU-T SG 13
– ITU-T SG 15
– ITU-T SG 20
– ITU-T SG 21
– ITU-D SG 1 and SG 2

Standardization bodies:

– IEC/TC 25, IEC/TC 25/JWG 1
– Institute of Electrical and Electronics Engineers (IEEE)
– Internet Engineering Task Force (IETF)
– ISO/IEC JTC 1/SCs 6, 17, 27 and 37
– ISO/TCs 12, 68, 215 and 307
– ISO/TC 12/JWG 20
– ETSI
– OASIS
– Kantara Initiative
– 3GPP

– Open wallet foundation
– EU digital identity wallet forum

Other bodies:

– International Bureau of Weights and Measures (BIPM)
– International Commission on Radiation Units and Measurements (ICRU)
– Fast Identity Online (FIDO) Alliance
– Open Id Foundation (OID)
– SIA (Secure Identity Alliance)
– SIDI Hub (Sustainable and Interoperable Digital Identity)
– International Labour Organization (ILO)
– World Health Organization (WHO)

WSIS Action Lines:

– C5

Sustainable Development Goals:

– 8, 9