Question 10/17 – Identity management and telebiometrics architecture and mechanisms

(Continuation of Question 10/17)

1 Motivation

Biometrics is gaining acceptance in applications performing but not limited to identity verification such as e-commerce, tele-medicine, and e-health. Biometric application systems present various challenges related to operational and technical data protection, reliability, and security of biometric data for biosafety and biosecurity applications.

Server-side biometric authentication becomes more complicated and demanding when biometric authentication is adopted in an open network environment. Telecommunication applications (such as telebiometrics) using mobile terminals and Internet services demand authentication methods to provide high security and friendly usage. It is necessary to specify requirements for the usage of telebiometric data in a manner that is safe, secure and with enhanced operational and data protection.

Identity management (IdM) is the management of the life cycle and use (creation, maintenance, utilization, and revocation) of credentials, identifiers, attributes, and patterns by which entities (e.g. service providers, end-user, organizations, network devices, applications, and services) are known with appropriate levels of trust. Depending on the context, multiple identities may exist for a single entity at differing security requirements, and at multiple locations. Depending on the identity model, the control over identities can be centralized or decentralized or a combination of both. In public networks, IdM supports trusted information exchange between authorized entities. The exchange is based on assertion of identities across distributed systems from multiple service providers. The exchange can also be based on various service environments such as cloud and 5G. IdM also improves the protection of private information and based on the trust model can ensure that only authorized information is disseminated.

IdM is a key component of telecommunications/ICT networks, services, and products because it supports establishing and maintaining trusted communications. In addition to performing authentication of an entity's identity, it also permits authorization of access based on privileges. It also supports the change of privileges when an entity's role changes delegation, and other identity-based services.

IdM is a critical component in managing network security because it improves assurance for the nomadic, on-demand access to networks and services that end-users expect. Along with other defensive mechanisms, IdM helps to prevent fraud and identity theft and thereby increases users' confidence that transactions are secure and reliable. As IdM works in a mutual manner, this increased level of trust applies equally to both the end user and service provider.

National/regional specific IdM specifications and solutions will exist and continue to evolve. Setup a foundation upon which harmonize solutions could be implemented is important. In addition to the study of telebiometric, this Question is dedicated to the vision setting and the coordination and organization of the entire range of IdM activities within ITU-T. A top-down approach to the IdM will be used with collaboration with other study groups and other standards development organizations (SDOs). It is recognized that other Questions will be involved in specific aspects of IdM, i.e. protocols, requirements, network device identifiers, etc.

Recommendations and Supplements under responsibility of this Question as of 7 January 2022: 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.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, and Supplements X.Suppl.7 and X.Suppl.35.

Texts under development as of 7 January 2022: X.1250rev, X.gpwd, X.oob-sa, X.pet_auth, X.srdidm, and X.tec-idms.

2 Question

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

a) How to further enhance or revise the current Recommendations for their wide deployment and usage?

b) What are the requirements for biometrics authentication in a high functionality network?

c) How should security countermeasures be assessed for particular applications of telebiometrics?

d) How should biometric systems and operations be developed in order to be conformant to the security requirements for any application of telebiometrics including cloud computing services?

e) How can identification and authentication of users be improved in the aspects of safety and security by the use of interoperable models in telebiometrics?

f) What mechanisms need to be supported to ensure safe and secure manipulation of biometric data in not only existing but also emerging application of telebiometrics, e.g., e-health, tele-medicine, e-commerce, online-banking, video surveillance?

g) How should biometric systems and operations be developed in order to be conformant to functional requirements for entity authentication of pet animals using telebiometrics?

h) What are the functional concepts for a common identity management (IdM) infrastructure?

i) What is an appropriate IdM model that is independent of network technologies, supports user-centric involvement, cloud-based identity, decentralized identity models and supports the secure exchange of IdM information between involved entities (e.g., users, relying parties and identity providers) based on consent and related policies?

j) What are the components of a generic framework and requirements for IdM?

k) What are the specific IdM requirements of service providers?

l) What are the requirements, capabilities, and possible strategies for achieving interoperability between different IdM systems (e.g., identity assurance, inter-working)?

m) What are the issues to consider supporting identity on distributed ledger technologies including wallet, decentralized identifiers and verifiable credentials?

n) What are the candidate mechanisms for IdM interoperability to include identifying and defining applicable profiles to minimize interoperability issues?

o) What are the requirements and mechanisms for the protection and disclosure of personally identifiable information (PII)?

p) How can an entity control its relationship when involved in identity-based relationships and interactions?

q) What are the requirements to protect IdM systems from cyber-attacks?

r) What IdM capabilities can be used against cyber-attacks?

s) How should IdM be integrated with advanced security technologies?

t) How can authentication be performed without shared secrets?

u) Can PKI based authentication be performed in an interoperable and secure manner?

v) Can biometric be used as part of strong authentication and trust layer to enable trusted interactions over a network?

w) What are the unique requirements for consumer-based identity management system in terms of identity vetting and account recovery without reliance on passwords?

x) How trust and relationship can be used to enhance account recovery, users' security and experience when dealing with relying parties?

3 Tasks

Tasks include, but are not limited to:

a) Enhance and revise current Recommendations of telebiometric authentication.

b) Review the similarities and differences among the existing telebiometrics Recommendations in ITU-T and standards in ISO/IEC.

c) Study and develop security requirements and guidelines for any application of telebiometrics using architectures and frameworks including the ones developed under Question 2/17.

d) Study and develop requirements for evaluating security and operational and technical data protection techniques for any application of telebiometrics.

e) Study and develop requirements for telebiometric applications in a high functionality network.

f) Study and develop integrated frameworks and requirements of telebiometric applications for cloud computing and data storage environments.

g) Study and develop requirements of telebiometric authentication for trust identity framework.

h) Study and develop requirements for appropriate generic protocols providing safety, security, operational and technical data protection, and consent "for manipulating biometric data" in any application of telebiometrics, e.g., e-health, tele-medicine, e-commerce, online-banking, e-payment, and video surveillance.

i) Study and develop Biology-to-Machine (B2M) protocols for transmitting biological metrics of which interoperate with Machine-to-Machine (M2M) protocols.

j) Study and develop telebiometric applications using bio-signals for applications including but not limited to authentication, identification, and health information monitoring.

k) Study and develop entity authentication services for pet animals based on telebiometrics.

l) Specify an IdM framework that supports discovery, policy and trust model, authentication and authorization, assertions, and credential lifecycle management required for IdM.

m) Define functional IdM architectural concepts to include IdM bridging between networks and among IdM systems, taking into account advanced security technologies.

n) Specify requirements (and propose mechanisms) for identity assurance, and mapping/interworking between different identity assurance methods that might be adopted in various networks. In this context, identity assurance includes identity patterns and reputation.

o) Define interfaces for interoperability of IdM systems.

p) Define requirements (and propose mechanisms) for protection and disclosure of personally identifiable information (PII).

q) Define requirements (and propose mechanisms) to protect IdM systems including how to use IdM capabilities as a means for service providers to coordinate and exchange information regarding cyber-attacks.

r) Maintain and coordinate IdM terminology and definitions living list.

s) Study and define IdM security risks and threats.

t) Study and develop decentralized identity management systems with support to user control of their identities.

u) Support of trusted identity management systems that can federate across systems, services, devices, IoT and applications.

v) Support identity management system providing identity management as a service for cloud agents, 5G networks and mobile devices.

w) 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.

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

4 Relationships

WSIS Action Lines:

– C5

Sustainable Development Goals:

– 8 (Decent Work and Economic Growth)

– 9 (Industry, Innovation and Infrastructure)

Recommendations:

– X- and Y-series

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

Questions:

– ITU-T Qs 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 11/17, 15/17, 7/13 and 14/15

Study Groups:

– ITU-D SG 1, SG2/2; ITU-R SG7; ITU-T SGs 2, 5, 9, 11, 13, 15, 16 and 20

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; 3GPP2

Other bodies:

– International Bureau of Weights and Measures (BIPM); International Commission on Radiation Units and Measurements (ICRU); Fast Identity Online (FIDO) Alliance; DID Alliance; International Labour Organization (ILO); World Health Organization (WHO)