|  |  |  |
| --- | --- | --- |
|  | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2022-2024 | SG17-LS25 |
| **STUDY GROUP 17** |
| **Original: English** |
| **Question(s):** | 10/17, All/17 | Geneva, 23 August - 2 September 2022 |
| **(Ref.:** [**SG17-TD601R1**](https://www.itu.int/md/T22-SG17-220823-TD-PLEN-0601/en)**)** |
| **Source:** | ITU-T Study Group 17 |
| **Title:** | LS on Coordination for Identity Management  |
| **LIAISON STATEMENT** |
| **For action to:** | FIDO Alliance, W3C DID WG, OASIS, RAISE Forum, NIST, ISO/IEC JTC 1/SC 27/WG 5, ISO/TC 307/WG 4, ITU-T SGs 2, 3, 5, 9, 11, 12, 13, 15, 16, 20 |
| **For information to:** | - |
| **Approval:** | ITU-T Study Group 17 meeting (Geneva, 2 September 2022) |
| **Deadline:** | 31 October 2022 |
| **Contact:** | Heung Youl YoumChairman of ITU-T SG17Co-chairman of JCA-IdM | E-mail: hyyoum@sch.ac.kr |
| **Contact:** | Keundug ParkCo-chairman of JCA-IdM | E-mail: jacepark926@gmail.com |
| **Contact:** | Abbie BarbirCo-chairman of JCA-IdM | E-mail: BarbirA@cvshealth.com |
| **Contact:** | Hiroshi TakechiCo-chairman of JCA-IdM  | E-mail: hiro@takechi.org  |

ITU-T Study Group 17 (SG17) thanks you for your continuous coordination and collaboration on identity management.

We are pleased to share with you the results of 30th JCA-IdM meeting which took place on 26 August 2022 in Annex A.

We are maintaining the IdM roadmap which provides an insight on standardization work in this area across the world. We identified some parts of this roadmap may need to be updated. We invite you to review the IdM roadmap related to your organization in Annex B and the IdM contact list in Annex C and to provide us with any updates.

SG17 also invites you to the 31th JCA-IdM meeting to share your activities on identity management, which will take place on Friday (24 February 2023) of first week during the SG17 meeting in February 2023.

We look forward to your further collaboration in this area.

**Annex A – Report of the 30th JCA-IdM meeting on Friday 26 August 2022**

The 30th JCA-IdM meeting was held in Geneva with remote participation during the SG17 meeting at 14:30-16:00 (CEST) on 26 August 2022. The meeting was chaired by Dr. Keundug Park, Co-chairman, and Prof. Heung Youl Youm, Co-chairman. The meeting started at 14:30 as scheduled. The co-chairman welcomed all participants.

34 participants attended the JCA-IdM meeting, see Attachment 1.

Documents are available at

* [http://www.itu.int/en/ITU-T/jca/idm](http://www.itu.int/en/ITU-T/jca/idm/)
* <https://www.itu.int/en/ITU-T/jca/idm/Pages/docs-2224.aspx> and
* [JCA-IdM DOC 199](https://www.itu.int/en/ITU-T/jca/idm/Documents/2022-2024/JCA-IDM-199.docx) provides information on the practical facilities available for the conduct of the work of JCA-IdM.
1. The co-chairmen gave opening remarks and introduced the participants. The meeting was started at 14:30 as scheduled. The co-chairman welcomed all participants
2. The agenda was discussed and adopted as provided in [JCA-IdM DOC 200R2](https://www.itu.int/en/ITU-T/jca/idm/Documents/2022-2024/JCA-IDM-200R2.docx).
3. Dr. Keundug Park presented the previous JCA-IdM meeting report: [JCA-IdM DOC 198](https://www.itu.int/en/ITU-T/jca/idm/Documents/2022-2024/JCA-IDM-198.docx). There was no comment, and the report was approved.
4. Ms. Shuguang Qi presented the Liaison Statement from ITU-T SG5 and mentioned ITU-T SG5 has no updates on IdM.
5. Mr. Salvatore Francomacaro provided ISO/TC 307/JWG 4 updates on ISO/TR 23249 (Overview of existing DLT systems for identity management), ISO/DTR 23644 (Overview of trust anchors for DLT-based identity management), ISO/PWI 12833 (Re-identification and privacy vulnerabilities and mitigation methods in blockchain and distributed ledger technologies), and ISO/AWI 7603 (Decentralized Identity standard for the identification of subjects and objects). He mentioned that ITU-T SG17/TC 307 joint workshop on “DLT security, identity management and privacy” would take place in February 2023.
6. Mr. Brent Zundel provided W3C verifiable credential working group (VCWG) updates on normative deliverables for example, Verifiable Credentials Data Model (VCDM) 2.0, Securing Verifiable Credentials (SVC) 1.0 and the other deliverables. He informed that the decentralized identifiers working group (DID WG) has drafted the next own charter and the VCWG has recently been rechartered.
7. Prof. Kai Rannenberg presented briefly ISO/IEC JTC 1/SC 27/WG 5 updates without the presentation slide deck.
8. Dr. Keundug Park provided ITU-T Q10/17 updates on ITU-T X.gpwd (Threat Analysis and guidelines for securing password and password-less authentication solutions), X.1250rev(Baseline capabilities for enhanced global identity management and interoperability), X.1251rev(A framework for user control of digital identity), X.pet\_auth (Entity authentication service for pet animals using telebiometrics), X.tec\_idms (Management and protection techniques for user data protection in distributed identity systems), X.oob-sa (Framework for out-of-band server authentication using mobile devices), and X.srdidm (Security requirements for decentralized identity management systems using distributed ledger technology). He informed ITU-T SG17 attended the 1st JCA-DCC (Joint Coordination Activity on Digital COVID-19 Certificates) meeting on 1 June 2022.
9. Dr. Keundug Park presented the revised JCA-IdM roadmap. There was no comment, and the meeting agreed to the revised roadmap.
10. The meeting was informed to send out Liaison Statement comprising this JCA-IdM meeting report, the updated IdM roadmap, and JCA-IdM contact lists to related groups.
11. All delegates expressed thanks to the organizer of JCA-IdM for giving opportunity to present and share their activities and works.
12. The meeting did not discuss the contact list, however, assumed to update, if necessary, contact list in [JCA-IdM DOC 0 Rev.10](https://www.itu.int/en/ITU-T/jca/idm/Documents/2022-2024/JCA-IDM-000-R10.docx).
13. The next JCA-IdM meeting will take place on Friday (24 February 2023) of first week during the SG17 meeting in February 2023. The invitation letter for this meeting will be sent to delegates after this JCA-IdM meeting.
14. The meeting agreed to circulate all presentation materials to the delegates after the JCA-IdM meeting.
15. The meeting appreciated all participants presenting update of their group and looks forward to future participation in the JCA-IdM.
16. The meeting was closed at 15:45.

**Attachment 1 – 30th JCA-IdM meeting participants**

|  |  |  |  |
| --- | --- | --- | --- |
|  | ***Name*** | ***Email*** | ***Affiliation/Representative*** |
| 1 | Abdneour Bourennane | abdenour.bourennane@algerietelecom.dz | - |
| 2 | Brent Zundel | brent.zundel@avast.com | W3C DID WG, Co-chairman |
| 3 | Byoungmoon Chin | bmchin@sch.ac.kr | - |
| 4 | Cheng Li | - | - |
| 5 | Daeun Hyeon | hde0610@naver.com | - |
| 6 | Dong Bin Choi | DBchoi85@gmail.com | - |
| 7 | f.samake | - | - |
| 8 | Gabriel Daniel Ndwete | gabrielndwete@gmail.com | - |
| 9 | Georges Sebek | georges.sebek@ties.itu.int | - |
| 10 | Greg Ratta | gratta@ntia.gov | - |
| 11 | Heung-Ryong Oh | [hroh@tta.or.kr](file:///C%3A%5CUsers%5Cbilani%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CContent.Outlook%5CPATC8GWA%5Chroh%40tta.or.kr) | Q2/17, Co-rapporteur |
| 12 | Heung Youl Youm | hyyoum@sch.ac.kr | JCA-IdM, Co-chairman |
| 13 | Hiroshi Takechi | hiro@takechi.org | JCA-IdM, Co-chairman |
| 14 | Jaenam Ko | freeinlove1127@gmail.com | - |
| 15 | Jinghua Min | minjinghua@qq.com | - |
| 16 | John Caras | john.caras@telebiometrics.com | Q10/17, Co-rapporteur |
| 17 | Jonghyun Woo | jhwoo@dualauth.com | - |
| 18 | Junhyung Park | chelues17@gmail.com | - |
| 19 | Kai Rannenberg | kai.rannenberg@m-chair.de | JTC 1/SC 27/WG 5, Convenor |
| 20 | Keundug Park | jacepark926@gmail.com | JCA-IdM, Co-chairman |
| 21 | Kwadwo Osafo-Maafo | kwadwo.osafo-maafo@nca.org.gh | ITU-T SG17, Vice-chairman |
| 22 | Kyeong Hee Oh | khoh@tcaservices.kr | Q14/17, Co-rapporteur |
| 23 | Mark McFadden | mark@internetpolicyadvisors.com | - |
| 24 | Masaki Nakamura | - | - |
| 25 | P.K.Singh | - | - |
| 26 | Salvatore Francomacaro | salvatore.francomacaro@nist.gov | ISO/TC 307/JWG 4, Co-convenor |
| 27 | Shuguang Qi | qishuguang@caict.ac.cn | ITU-T SG5, Vice-chairman |
| 28 | Sungchae Park | zoesc.park@sch.ac.kr | JCA-DCC, Editor of roadmap |
| 29 | Takamasa Isohara | - | - |
| 30 | Tony Holmes | tonyarholmes@btinternet.com | - |
| 31 | Vincent Mwesigwa | vmwesigwa@ucc.co.ug |  |
| 32 | Xiaoya Yang | xiaoya.yang@itu.int | ITU-T SG17, Counsellor |
| 33 | Youngjoo Lee | yjoo99@hanmail.net | - |
| 34 | Zhiyuan Hu | huzhiyuan@vivo.com | WP2/17, Vice-chairman |

**Annex B – IdM roadmap**

This part of the roadmap provides information about identity management-related activities and documents from the ITU-T and from other standard organizations. Information is organized to reflect the activities, the resulting products and the various stages of development. The overall objective is to enable users of this part of the Roadmap to gain a thorough understanding of the IdM work by providing a comprehensive overview of the requirements driving the activities as well as by identifying the organizations involved, their inter-relationships and the status of their work.

The identity management work of ETSI, FIDO Alliance, IETF, ISO/IEC, ITU, NIST, Open Identity Exchange, Kantara Initiative and 3GPP is currently included in this part of the Roadmap. Further expansion to other organizations is anticipated as data is made available.

Summaries of the IdM standards work in progress are included below by identifying the respective organizations and their overall work programs. In addition, this part of the Roadmap includes a section devoted to the very important topic of national IdM strategies. In general, information in the body of the roadmap is in the form of brief summaries and headings; more detailed information may be obtained by following the hot links.

**1. Key international and regional IdM standards development and deployment activities (including approved standards and work items under development)**

**1.1 ITU-T**

Identity Management work in ITU-T is concentrated in seven Study Groups: SG2, SG3, SG11, SG13, SG16, SG17 and SG20. SG17 has been designated the Lead Study Group on Identity Management.

**SG17 (Security)**

In SG17, identity management work is the primary Identity management architecture and mechanisms. The following work has been completed in Question 10.

[X.1250: Baseline capabilities for enhanced global identity management and interoperability](https://www.itu.int/rec/T-REC-X.1250-200909-I)

[X.1251: A framework for user control of digital identity](https://www.itu.int/rec/T-REC-X.1251-200909-I)

[X.1252: Baseline identity management terms and definitions](https://www.itu.int/rec/T-REC-X.1252/en)

[X.1253: Security guidelines for identity management systems](https://www.itu.int/rec/T-REC-X.1253/en)

[X.1254: Entity authentication assurance framework](https://www.itu.int/rec/T-REC-X.1254)

[X.1255: Framework for discovery of identity management information](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11951)

[X.1256: Guidelines and framework for sharing network authentication results with service applications](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12605)

[X.1257: Identity and access management taxonomy](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12608)

[X.1258: Enhanced entity authentication based on aggregated attributes](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12850)

[X.1261\*: Policy framework including principles for digital identity infrastructure](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14270)

\*Dual numbering of the [D.267](https://www.itu.int/rec/T-REC-D.267) (SG3) as [X.1261](https://www.itu.int/rec/T-REC-X.1261/_page.print) (SG17)

[X.1275: Guidelines on protection of personally identifiable information in the application of RFID technology](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=10441)

[X.1276: Authentication step-up protocol and metadata Version 1.0](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13606)

[X.1277: Universal authentication framework](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13727)

[X.1278: Client to authenticator protocol/Universal 2-factor framework](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13728)

[X.1279: Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14261)

[X.1365](https://www.itu.int/rec/T-REC-X.1365-202003-P) (X.ibc-iot): Security framework for use of identity-based cryptography in support of IoT services over telecom networks

[X.Sup7: **ITU-T X.1250 series -** Supplement on overview of identity management in the context of cybersecurity](https://www.itu.int/rec/T-REC-X.Sup7-200902-I)

[X Suppl. 22: ITU-T X.1144 *-* Supplement on enhancements and new features in eXtensible Access Control Markup Language (XACML 3.0)](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12156)

[X Suppl. 35: ITU-T X.1254 – Supplement on use cases of entity authentication assurance (EAA) framework](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14066)

Work in progress includes:

[X.1250rev](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16762): Baseline capabilities for enhanced global identity management and interoperability

[X.1251rev](https://www.itu.int/md/T17-SG17-210420-TD-PLEN-3704/en): A framework for user control of digital identity

[X.gpwd](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16770): Threat Analysis and guidelines for securing password and password-less authentication solutions

X.oob-sa: Framework for out-of-band server authentication using mobile devices

X.pet\_auth: Entity authentication service for pet animals using telebiometrics

X.srdidm: Security requirements for decentralized identity management systems using distributed ledger technology

**SG2 (**[**Operational aspects**](https://www.itu.int/en/ITU-T/studygroups/2017-2020/02/Pages/default.aspx)**)**

The following work has been completed:

[E.217](https://www.itu.int/rec/T-REC-E.217/en): Maritime communications - Ship Station identity

Work in progress includes:

[TR.OTTnum](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15041): Current use of E.164 numbers as identifiers for OTTs

[E.sup.OTTnum](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=15042): Guidance on the use of E.164 numbers as identifiers for OTTs

[E.IoT-NNAI](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=13968): Internet of Things Naming Numbering Addressing and Identifiers

M.uiamr: User Identity and Access Management Requirements for Telecommunications Management Network

**SG3 (**[**Economic and policy issues**](https://www.itu.int/en/ITU-T/studygroups/2013-2016/03/Pages/default.aspx)**)**

The following work has been completed:

[D.1140](https://www.itu.int/rec/T-REC-D.1140/_page.print) (D.DigID)| [X.1261](https://www.itu.int/rec/T-REC-X.1261/_page.print)\*: Policy framework including principles for digital identity infrastructure

\*Dual numbering of the D.1140 (SG3) as [X.1261](https://www.itu.int/rec/T-REC-X.1261/_page.print)(SG17)

Work in progress includes:

[D.princip\_bigdata](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18189): Policy framework and principles for data protection in the context of big data relating to international telecommunication services

[Study\_bigdata](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18183): Technical Paper on economic and policy aspects of Big Data in international telecommunication services and networks

**SG11 (Protocols, testing & combating counterfeiting)**

In SG11, identity management related work is undertaken by Question 2, Question 12, and Question 15 as follows:

a) Q2/11: Identity management on telecommunication equipment (such as trustable interconnection between network entities) and service (such as calling party line identity);

b) Q12/11: Identity management related to test of internet of things;

c) Q15/11: Identity management on combating counterfeit and stolen telecommunication/ICT devices.

The following work has been completed:

[Q.5052 (ex Q.DEV\_DUI)](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15223) : Addressing mobile devices with duplicate unique identifier

Q.3062 (ex Q.Pro-Trust): Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks

Q.3063 (ex Q.CIDA): Signalling procedures of calling line identification authentication

**SG13 (Future Networks)**

In SG13, identity management related work is undertaken by Question 22 (Networks beyond IMT2020: Emerging network technologies).

The following work has been completed:

[Y.2720: NGN identity management framework](https://www.itu.int/rec/T-REC-Y.2720-200901-I)

[Y.2721: NGN identity management requirements and use cases](https://www.itu.int/rec/T-REC-Y.2721-201009-I)

[Y.2722: NGN identity management mechanisms](https://www.itu.int/rec/T-REC-Y.2722-201101-I)

Work in progress includes:

[Y.SCid-fr](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16491): Requirements and converged framework of self-controlled identity based on blockchain

**SG16 (Multimedia and digital technologies)**

The following work has been completed:

[H.642.3](https://www.itu.int/rec/T-REC-H.642.3/en): Information technology – Automatic identification and data capture technique - Identifier resolution protocol for multimedia information access triggered by tag-based identification

**SG20 (IoT, smart cities & communities)**

In SG20, identity management related work is undertaken by Question 6.

Work in managing includes:

H.642.3: Information technology – Automatic identification and data capture technique – Identifier resolution protocol for multimedia information access triggered by tag-based identification

The following work has been completed:

[Y.4462](https://www.itu.int/rec/T-REC-Y.4462/en) (Y.IoT-ics): Requirements and functional architecture of open IoT identity correlation service

Y.4809 (ex Y.IoT-ITS-ID): Unified IoT Identifiers for intelligent transport systems

Y.4476 (ex Y.IoT-rf-dlt): OID-based Resolution framework for transaction of distributed ledger assigned to IoT resources

[Y.4811](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14821): Reference framework of converged service for identification and authentication for IoT devices in a decentralized environment

[Y.4500.3 (ex Y.oneM2M.SEC.SOL](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17890)): oneM2M - Security Solutions

Work in progress includes:

[Y.IoT-Smartcity-Risk](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17916): Reference framework of cybersecurity risk management of IoT ecosystems on smart cities

[YSTR-IADIoT](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17917): Intelligent Anomaly Detection System for IoT

[Y.IoT-IoD-PT](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17884): Identity of IoT devices based on secure procedures and ensures privacy and trust of IoT systems

[YSTR.Feas-DID-IoT](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17909): Feasibility of Decentralised Identifiers (DIDs) in IoT

[Y.FW.IC.MDSC](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17888): Framework of identification and connectivity of moving devices in smart city

[Y.IoT-Ath-SC](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17895): Framework of IoT-devices authentication in smart city

YSTR.IoT-IMS: Requirements and capability framework for identification management service of IoT device

**1.2 ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection)**

The following work has been completed:

[ITU-T X.1085](https://www.itu.int/rec/T-REC-X.1085/_page.print) | [ISO/IEC 17922](file:///C%3A%5CUsers%5Chbert%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CContent.Outlook%5CZPH2TK3M%5CISO%5CIEC%2017922)  Telebiometric authentication framework using biometric hardware security module was published as an International Standard (IS) in 2017-09 as common text with ITU-T.

[ISO/IEC 20547-4](https://www.iso.org/standard/71278.html) – Big data reference architecture – Part 4: Security and privacy was published as an International Standard (IS) in 2020-09.

[ISO/IEC 20889](https://www.iso.org/standard/69373.html) – Privacy enhancing data de-identification terminology and classification of techniques was published as an International Standard (IS) in 2018-11.

[ISO/IEC 24745](https://www.iso.org/standard/52946.html) – Biometric information protection was published as an International Standard (IS) in 2011-06. A revision h has been progressed to DIS status.

[ISO/IEC 24760](https://www.iso.org/standard/77582.html) – A Framework for identity management: Part 1 “Terminology and Concepts” was published as a second edition in 2019-05.It is freely available at no cost via www.jtc1.org

[ISO/IEC 24761](https://www.iso.org/standard/71163.html) – Authentication context for biometrics was published as a second edition International Standard (IS) in 2019-10

[ISO/IEC TS 27006-2](https://www.iso.org/standard/71676.html) (formerly 27558) – Requirements for bodies providing audit and certification of information security management systems – Part 2: Privacy Information Management Systems was published as a Technical Specification (TS) in 2021-02

[ISO/IEC 27018](https://www.iso.org/standard/76559.html) – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors was first published as an International Standard (IS) in 2014-08. A minor revision was published in 2019-01.

[ISO/IEC TR 27550](https://www.iso.org/standard/72024.html) – Privacy engineering for system life cycle processes was published as a Technical Report (TR) in 2019-09.

ISO/IEC 27551 – Requirements for attribute-based unlinkable entity authentication was published as an International Standard (IS) in 2021-09

ISO/IEC 27555 –Guidelines on personally identifiable information deletion has been published as an International Standard (IS) in 2021-10.

[ISO/IEC TS 27570](https://www.iso.org/standard/71678.html) – Privacy guidelines for smart cities was published as a Technical Specification (TS) in 2021-02.

[ISO/IEC 27701](https://www.iso.org/standard/71670.html) (formerly 27552) – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines was published as an International Standard (IS) in 2019-08.

[ISO/IEC TS 29003](https://www.iso.org/standard/62290.html) – Identity proofing was published as a Technical Specification (TS) in 2018-03. For the upcoming Systematic Review SC 27 recommends conformation.

[ISO/IEC 29100](https://www.iso.org/standard/45123.html) – Privacy framework was published as an International Standard (IS) in 2011-12 An Amendment was published in 2018. It is freely available at no cost via www.jtc1.org.

[ISO/IEC 29101](https://www.iso.org/standard/75293.html) – Privacy architecture framework was first published as an International Standard (IS) in 2013-10. A minor revision was published in 2018-11.

[ISO/IEC 29115](https://www.iso.org/standard/45138.html) – Entity authentication assurance framework was published as an International Standard (IS) in 2013-04.

[ISO/IEC 29134](https://www.iso.org/standard/62289.html) – Guidelines for privacy impact assessment was published as an International Standard (IS) in 2017-06.

[ISO/IEC 29146](https://www.iso.org/standard/45169.html) – A framework for access management was published as an International Standard (IS) in 2016-06.

[ITU-T X.1058](https://www.itu.int/rec/T-REC-X.1058/en) | [ISO/IEC 29151](https://www.iso.org/standard/62726.html) – Code of practice for personally identifiable information protection was published as an International Standard (IS) in 2017-08 as common text with ITU-T.

[ISO/IEC 29184](https://www.iso.org/standard/70331.html) – Online privacy notices and consent was published as an International Standard (IS) in 2020-06.

[ISO/IEC 29190](https://www.iso.org/standard/45269.html) – Privacy capability assessment model was published as an International Standard (IS) in 2015-08. For the upcoming Systematic Review SC 27 recommends conformation.

[ISO/IEC 29191](https://www.iso.org/standard/45270.html) – Requirements for partially anonymous, partially unlinkable authentication was published as an International Standard (IS) in 2012-12 and confirmed in 2018-11.

Work in progress includes:

ISO/IEC TS 27006-2 (formerly 27558) – Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy Information Management Systems has been published as an International Standard (IS) in 2021-02. A revision in preparation for an International Standard (IS) has been initiated and was progressed to Committee Draft (CD) status.

ISO/IEC 27553 – Security and privacy requirements for authentication using biometrics on mobile devices, is divided in two parts, Part 1: Local mode, and Part 2: Remote mode. Work on Part 1 had been progressed to Draft International Standard (DIS) status. Due to a failure in the ballot system the ballot deadline needed to be extended, so the work on the DIS ballot results will only happen in a special meeting on 2022-05-23/25. Work on Part 2 has been progressed to a New Work Item Ballot.

ISO/IEC 27554 – Application of ISO 31000 for assessment of identity management-related risk is undergoing a title change to Application of ISO 31000 for assessment of identity-related risk and remains at Committee Draft (CD) status.

ISO/IEC 27556 – User-centric framework for PII handling based on privacy preferences was undergoing a title change to User-centric privacy preferences management framework and had been progressed to Draft International Standard (DIS) status. Due to a failure in the ballot system the ballot deadline needed to be extended, so the work on the DIS ballot results will only happen in a special meeting on 2022-05-23/25.

ISO/IEC 27557 – Organizational privacy risk management had been progressed to Draft International Standard (DIS) status. Due to a failure in the ballot system the ballot deadline needed to be extended, so the work on the DIS ballot results will only happen in a special meeting on 2022-05-23/25.

ISO/IEC 27559 – Privacy-enhancing data de-identification framework had been progressed to Draft International Standard (DIS) status. Due to a failure in the ballot system the ballot deadline needed to be extended, so the work on the DIS ballot results will only happen in a special meeting on 2022-05-30.

ISO/IEC 27560 – Consent record information structure remains at Working Draft (WD) status.

ISO/IEC 27561 – Privacy operationalization model and method for engineering (POMME) was progressed to Committee Draft (CD) status pending approval of document type from TS to IS.

ISO/IEC 27562 – Privacy guidelines for fintech services remains at Working Draft (WD) status.

ISO/IEC 27563 – Impact of security and privacy in artificial intelligence use cases has been progressed to Draft Technical Report (DTR) stage. It is awaiting approval of a title change to Security and privacy in artificial intelligence use cases.

ISO/IEC 27565 – Guidelines on privacy preservation based on zero knowledge proofs has been approved as a New Project (NP) and was progressed to Working Draft (WD) status.

**WG 5 PWI:**

PWI 6087 – Digital authentication: Risks and mitigations was initiated in 2020-09 and is on-going.

PWI 6089 – Impact of AI on security and privacy was started in 2020-09 and is on-going.

PWI 6102 – Guidance on illustrative processes of a privacy information system was initiated in 2020-09 and is on-going.

PWI 7732 – Age verification was initiated in 2021-04 and is on-going.

PWI 7748 – Framework for Privacy Preservation based on Zero-Knowledge Proofs was initiated in 2021-04 and has been completed by proposing a New Work Item Proposal (NWIP).

PWI 24760-4 – A Framework for identity management: Part 4 “Terminology and Concepts” Authenticators, credentials and authentication has been initiated.

PWI 27564 – Privacy models has been initiated.

**WG 5 Standing documents (SD):**

WG 5 SD1 Roadmap is available via the website of JTC 1/SC 27 at www.din.de/en/meta/jtc1sc27/downloads and will be updated reflecting expert contributions and the progress at the WG meeting.

WG 5 SD2 Privacy References List is available via the website of JTC 1/SC 27 at www.din.de/en/meta/jtc1sc27/downloads and will be updated based on contributions received.

WG 5 SD4 Standards Privacy Assessment is available via the website of JTC 1/SC 27 at www.din.de/en/meta/jtc1sc27/downloads and will be updated based on contributions received.

**1.3 ISO/TC 307 and ISO/IEC JTC 1/SC 27/WG 5 and JWG 4:**

The most relevant ISO activity related to IdM is TC 307 - Blockchain and distributed ledger technologies, created in 2016 and whose scope is “Standardisation of blockchain technologies and distributed ledger technologies.”

TC 307 has ISO/TC 307/JWG 4 on Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27/WG 5: Security, privacy and identity for Blockchain and DLT".

The following work has been completed:

[ISO 22739:2020](https://www.iso.org/standard/73771.html) Blockchain and distributed ledger technologies — Vocabulary was published as an International Standard (IS) in 2020-07

ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations was published as a Technical Report (TR) in 2020-05

Work in progress includes:

[ISO/TR 23249](https://www.iso.org/standard/80805.html) Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management is currently under publication

[ISO/WD TR 23642](https://www.iso.org/standard/81772.html) Blockchain and distributed ledger technologies - Overview of smart contract security good practice and issues is currently at WD status

[ISO/DTR 23644](https://www.iso.org/standard/81773.html) Blockchain and distributed ledger technologies - Blockchain and distributed ledger technologies - Overview of trust anchors for DLT-based identity management (TADIM) will be published end of 2022

[ISO/AWI 7603](https://www.iso.org/standard/82842.html?browse=tc) Decentralized Identity standard for the identification of subjects and objects is currently at AWI status

ISO/PWI 12833 Re-identification and privacy vulnerabilities and mitigation methods in blockchain and distributed ledger technologies is currently at PWI status

**1.4 World Wide Web Consortium (W3C)**

The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards. W3C's mission is, in their words, to lead the Web to its full potential.

W3C has several activities that are relevant for IdM:

**Web Authentication WG**

The Web Authentication WG (end date: 15/09/2019) aims to define a client-side (i.e. in the browsers) API providing strong authentication functionality to Web Applications, obviating the limitations of password-based logins (weak security, vulnerable to phishing attacks, not usable).

The following work has been completed:

[An API for accessing Public Key Credentials, Level 2](https://www.w3.org/TR/2021/REC-webauthn-2-20210408/) on 8 April 2021.

**Decentralized Identifiers WG**

The recently started Decentralized Identifiers WG (DID, end date: 15/04/2021) has been proposed to enable identifiers that (from their charter):

1. are controlled by individuals, organizations, and machines, not leased from an authority (e.g. DNS Registrars).

2. are cryptographically verifiable and can authenticate their owners (e.g. DID- based website login).

3. are dereferenceable. i.e. they can be dereferenced to a document that provides information on how to start a secure and privacy preserving communication with the owner (e.g. a set of public keys and a set of service endpoints).

The WG will focus on the following points:

1. Define the DID URI scheme.

2. Recommend a data model and syntax(es) for the expression of Decentralized Identifier Documents, including one or more core vocabularies.

The following work has been completed:

[Decentralized Identifiers (DIDs) v1.0](https://www.w3.org/TR/did-core/)

**Verifiable Claims WG**

The Verifiable Claims WG (end date: 30/09/2019) aims at creating a standard that makes it easy for users to assert their verifiable qualifications to a service provider (e.g. my loyalty card number is X, I have an account at Bank Y, I am over the age of 21, I am a citizen of the USA, I have a degree in Mathematics, etc.). Such standard would allow expressing, exchanging, and verifying claims on the Web more easily and securely, across different industry sectors, and independently from a particular claim provider.

The following work has been completed:

[Verifiable Credentials Data Model 1.0](https://www.w3.org/TR/vc-data-model/)

**Data Privacy Vocabularies and Controls CG**

The mission of the W3C Data Privacy Vocabularies and Controls CG (DPVCG) is to develop a taxonomy of privacy terms, which include terms from the new European General Data Protection Regulation (GDPR). The aim is to provide a machine-readable vocabulary to annotate and categorize instances of legally compliant personal data processing according to the GDPR.

The taxonomy currently discussed in the group contains terms (classes and properties) related to the following concepts (corresponding to GDPR concepts):

* Personal Data Categories
* Purposes
* Processing Categories
* Technical and Organisational Measures
* Legal Basis
* Consent
* Recipients, Data Controllers, Data Subjects

Work in progress includes:

[Data Protection Aspects of Online Shopping – A Use Case](https://www.w3.org/community/dpvcg/2019/12/12/data-protection-aspects-of-online-shopping-a-use-case/)

**1.5 NIST**

Under the Systems and Emerging Technologies Security Research grouping, NIST has established a program on Personal Identity Verification of Federal Employees and Contractors.

The following technical publications have been developed:

NIST Special Publication 800-63-3, [Digital Identity Guidelines](https://csrc.nist.gov/publications/detail/sp/800-63/3/final)

NIST Special Publication 800-63A, [Digital Identity Guidelines: Enrollment and Identity Proofing](https://csrc.nist.gov/publications/detail/sp/800-63a/final)

NIST Special Publication 800-63B, [Digital Identity Guidelines: Authentication and Lifecycle Management](https://csrc.nist.gov/publications/detail/sp/800-63b/final)

NIST Special Publication 800-63C, [Digital Identity Guidelines: Federation and Assertions](https://csrc.nist.gov/publications/detail/sp/800-63c/final)

[NIST Special Publication 800-73](https://csrc.nist.gov/publications/detail/sp/800-73/4/final)-4, "Interfaces for Personal Identity Verification" specifies the interface and data elements of the PIV card.

[NIST Special Publication 800-76](https://csrc.nist.gov/publications/detail/sp/800-76/2/final), Biometric Data Specification for Personal Identity Verification" specifies the technical acquisition and formatting requirements for biometric data of the PIV system.

[NIST Special Publication 800-78](https://csrc.nist.gov/publications/detail/sp/800-78/4/final)-4, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification" specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system.

NIST Special Publication 800-157, [Guidelines for Derived Personal Identity Verification (PIV) Credentials](https://csrc.nist.gov/publications/detail/sp/800-157/final)

NIST Special Publication 800-178, [A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)](https://csrc.nist.gov/publications/detail/sp/800-178/final)

NIST Special Publication 1800-3, [Attribute Based Access Control (2nd Draft)](https://csrc.nist.gov/publications/detail/sp/1800-3/draft)

NIST Special Publication 1800-12, [Derived Personal Identity Verification (PIV) Credentials](https://csrc.nist.gov/publications/detail/sp/1800-12/final)

NIST Special Publication 1800-17, [Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers](https://csrc.nist.gov/publications/detail/sp/1800-17/final)

For the latest versions and revisions of the above NIST publications please see <http://csrc.nist.gov/publications/PubsSPs.html>.

**1.6 FIDO Alliance**

[**FIDO2 SPECIFICATIONS**](https://fidoalliance.org/specifications/download/)

[CLIENT TO AUTHENTICATOR PROTOCOL (CTAP)](https://fidoalliance.org/specifications/download/)

[W3C - Web Authentication: An API for accessing Public Key Credentials Level 1 (Webauthn)](https://fidoalliance.org/specifications/download/)

**UAF SPECIFICATIONS**

[FIDO UAF Complete Specifications](https://fidoalliance.org/specifications/download/)

[FIDO UAF Architectural Overview](https://fidoalliance.org/specifications/download/)

[FIDO UAF Protocol Specification](https://fidoalliance.org/specifications/download/)

[UAF Application API and Transport Binding Specification](https://fidoalliance.org/specifications/download/)

[FIDO UAF Authenticator-specific Module API](https://fidoalliance.org/specifications/download/)

[FIDO UAF Authenticator Commands](https://fidoalliance.org/specifications/download/)

[FIDO ECDAA Algorithm](https://fidoalliance.org/specifications/download/)

[FIDO UAF APDU Commands](https://fidoalliance.org/specifications/download/)

[UAF Registry of Predefined Values](https://fidoalliance.org/specifications/download/)

[FIDO UAF Android Protected Confirmation Assertion Format](https://fidoalliance.org/specifications/download/)

[FIDO UAF Web Authentication Assertion Format](https://fidoalliance.org/specifications/download/)

[FIDO UAF Readme](https://fidoalliance.org/specifications/download/)

[FIDO UAF ERRATA](https://fidoalliance.org/specifications/download/)

FIDO2 AND UAF COMMON FILES

[FIDO Authenticator Metadata Statements](https://fidoalliance.org/specifications/download/)

[FIDO Authenticator Metadata Service](https://fidoalliance.org/specifications/download/)

[FIDO Registry of Predefined Values](https://fidoalliance.org/specifications/download/)

[FIDO AppID and Facet Specification](https://fidoalliance.org/specifications/download/)

[FIDO Security Reference](https://fidoalliance.org/specifications/download/)

[FIDO Technical Glossary](https://fidoalliance.org/specifications/download/)

U2F SPECIFICATIONS

[FIDO U2F Complete Specifications](https://fidoalliance.org/specifications/download/)

[FIDO U2F Architectural Overview](https://fidoalliance.org/specifications/download/)

[FIDO U2F JavaScript API](https://fidoalliance.org/specifications/download/)

[FIDO U2F Raw Message Formats](https://fidoalliance.org/specifications/download/)

[FIDO U2F HID Protocol](https://fidoalliance.org/specifications/download/)

[FIDO U2F Bluetooth® protocol](https://fidoalliance.org/specifications/download/)

[FIDO U2F NFC protocol](https://fidoalliance.org/specifications/download/)

[FIDO U2F Transport Extensions](https://fidoalliance.org/specifications/download/)

[FIDO U2F Implementation Considerations](https://fidoalliance.org/specifications/download/)

[FIDO AppID and Facet Specification](https://fidoalliance.org/specifications/download/)

[FIDO Security Reference](https://fidoalliance.org/specifications/download/)

[FIDO Technical Glossary](https://fidoalliance.org/specifications/download/)

[FIDO U2F Readme](https://fidoalliance.org/specifications/download/)

The latest versions of the FIDO Alliance user authentication specifications are available here. See https://fidoalliance.org/specifications/download/

**2. Gap analysis on IdM standard development activities**

In the existing IdM standardization efforts there appear to be two clear trends. One trend is the drive for federation and interoperability, mainly pushed by the Liberty Alliance and OASIS. The efforts in the standardization of web services have matured quite well, primarily through the work of Liberty Alliance but also through the OASIS work. The development of federation standards for the general information system sector and the telecom sector is included in current and planned work of both ITU-T and ISO/IEC. The big issue associated with federation is interoperability and harmonization of the different federation stands and solutions. The second trend is the drift from standards for organization-centric identity management systems towards a more deliberate suit of standards trying to find a reasonable balance between end users need for security and privacy and the organization or business needs for security and information.

**3. Approved IdM standards**

Approved and published IdM standards are included in the database of standards included in [Part 2](https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/ict-part02.aspx) of this Roadmap.

Recent developments in IdM standards are addressed in the [IdM landscape wiki](http://groups.itu.int/Default.aspx?tabid=961&topic=IdM+Landscape), which contains informal and evolving information as well as in [Part 3](https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/ict-part03.aspx) of this Roadmap under the Programs of Work of the various standards bodies.

**4. Best practices**

[**ENISA**](https://www.enisa.europa.eu/%40%40search?Subject%3Alist=eID)[Mobile identity management (April 2010)](https://www.enisa.europa.eu/publications/Mobile%20IDM/at_download/fullReport)

This position paper reports on information security risks and best-practice in the area of Mobile Identity Management (Mobile IDM). It also provides recommendations of systems, protocols and/or approaches to address these challenges.

# Identity Management, Electronic Authentication and Secure Development

[Remote ID Proofing — ENISA](https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing) (March 11, 2021)

EC [Progress report on standardisation activities and technical sustainability plans](https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c65aea82&appId=PPGMS) (August 2019)

**5. Identity management in cloud computing**

[OASIS Identity in the Cloud](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=id-cloud) (The Technical Committee was closed by the OASIS TC Administrator on 07 November 2016)

**6. National identity management strategies**

[Next steps outlined for UK’s use of digital identity](https://www.gov.uk/government/news/next-steps-outlined-for-uks-use-of-digital-identity) (September 2020)

[National strategy for trusted identities in cyberspace draft (U.S)](https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf) (APRIL 2011)

[Open Identity Exchange (U.S)](http://openidentityexchange.org/) (14th October 2021)

[NSW Government Identity Strategy](https://www.nsw.gov.au/strategy/nsw-government-identity-strategy)(AU)

**7. Other relevant IdM activities and papers**

**Bibliography**

**Annex C – IdM contact list**

|  |  |  |
| --- | --- | --- |
| **Group** | **Contact** | **E-mail** |
| TSAG | VACANT |  |
| ITU-T SG2 | - Phil RushtonChairman of ITU-T SG2 | philrushton@rcc-uk.uk |
| ITU-T SG3 | - S. K. Mishra (Mr)Rapporteur of Q11/3 | shailendrakm@gmail.com |
| ITU-T SG5 | - Shuguang Qi (Ms)Vice-Chairman of ITU-T SG5 | qishuguang@caict.ac.cn |
| ITU-T SG9 | VACANT |  |
| ITU-T SG11 | - Cheng Li (Mr)Rapporteur of Q2/11 | licheng@caict.ac.cn |
| ITU-T SG12 | VACANT |  |
| ITU-T SG13 | VACANT |  |
| ITU-T SG15 | VACANT |  |
| ITU-T SG16 | - Sarra RebhiVice-chairman of ITU-T SG16 | rebhi.sarra@telediffusion.net.tn |
| ITU-T SG17 | - Keundug Park (Mr)Associate Rapporteur of Q10/17 | jacepark926@gmail.com  |
| - Heung Youl Youm (Mr)Chairman of ITU-T SG17 | hyyoum@sch.ac.kr  |
| ITU-T SG20 | VACANT |  |
| FIDO Alliance | - David Turner (Mr)Director of Standards Development | david@fidoalliance.org  |
| ISO/TC 307/JWG 4 | - Julien Bringer (Mr)Co-convenor of TC 307/JWG 4 | julien@kallistech.com  |
| ISO/IEC JTC 1/SC 27/ WG 5 | - Kai Rannenberg (Mr)Convenor of WG 5 | kai.rannenberg@m-chair.de  |
| NIST | - David Temoshok (Mr)Senior Advisor of NIST | david.temoshok@nist.gov  |
| RAISE Forum | - Meng-Chow Kang (Mr)Co-chairman of RAISE Forum/ AWS | mengchow.kang@gmail.com  |
| W3C DID WG | - Brent Zundel (Mr)Co-chairman of W3C DID WG | brent.zundel@avast.com |

**Annex D – Revised terms of reference for Joint Coordination Activity on Identity Management (JCA-IdM)**

**1 Scope**

WTSA-20 designated SG17 as the lead study group for identity management. The Terms of Reference of this JCA are consistent with clause 5.1 of Recommendation ITU-T A.1.

The scope of the JCA is coordination of the ITU-T identity management (IdM) work with internal and relevant external organizations. The term IdM is defined in Recommendation ITU-T X.1252. The Decentralized identity is described in B.1 of the Annex B in Recommendation ITU-T X.1252.

**2 Objectives**

* The JCA-IdM will ensure that the ITU-T IdM work including decentralized identity management, is progressed in a well-coordinated way between study groups, in particular with SG2, SG13, SG20 and SG17. Planning issues can be brought to the attention of the JCA-IdM. The JCA-IdM will facilitate work assignment through the involved study groups when it is not clear under which Question work should be done and recommend an allocation of tasks.
* The JCA-IdM will analyze IdM standardization items and coordinate an associated roadmap with ITU-T Q10/17.
* The JCA-IdM will act as a point of contact within ITU-T and with other SDOs/Fora on IdM, such as FIDO alliance, ISO/IEC JTC 1/SC 27/WG 5, W3C, and ISO/TC 307, in order to avoid duplication of work and assist in implementing the IdM tasks assigned by WTSA-20 Resolution 2 and in coordinating the implementation of GSC-16 Resolution 4 on identity management.
* In carrying out the JCA-IdM’s internal coordinating role, participants in the JCA-IdM will include representatives of relevant ITU-T study groups and other ITU groups. A portion of each JCA-IdM meeting may be allocated to raising awareness of IdM issues addressed by other ITU-T Study Groups Questions, and external organizations.
* In carrying out the JCA-IdM’s external collaboration role, representatives from other relevant recognized SDOs/Fora and regional/national organizations may be invited to join the JCA-IdM.

**3 Administrative support**

See clause 5.9 of Recommendation ITU-T A.1.​

**4 Meetings**

See clause 5.5 of Recommendation ITU-T A.1.

**5 Progress reports**

The JCA-IdM will report to SG17 at its meetings. Progress reports and proposals may be sent to relevant study groups as necessary, in accordance with Recommendation ITU-T A.1, clause 5.7.

**6 Leadership (Co-chairmen)**

Mr Abbie Barbir

Mr Hiroshi Takechi

Mr Keundug Park

Mr Heung Youl Youm

**7 Other contacts**

   JCA-IdM secretariat

   tsbidm@itu.int

**8 Lifetime**

See clause 5.10 of Recommendation ITU-T A.1.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_