|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | INTERNATIONAL TELECOMMUNICATION UNION  **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2022-2024 | | JCA-DCC-034R1 | | |
| JCA-DCC | | |
| Original: English | | |
|  | |  | | E-meeting, 2 December 2022 | |
| **DOCUMENT** | | | | | |
| **Source:** | | Editors of DCC standards roadmap, Chairman of JCA-DCC | | | |
| **Title:** | | Digital COVID 19 Certificates (DCC) Standardization Roadmap | | | |
| **Contact:** | | Sungchae Park Editor of JCA-DCC Soonchunhyang University Korea (Republic of) | | | Tel: +82-41-530-1328 E-mail: [zoesc.park@sch.ac.kr](mailto:zoesc.park@sch.ac.kr) |
| **Contact:** | | Keundug Park Editor of JCA-DCC Korea (Republic of) | | | Tel: +82-2-2182-6011 E-mail: [jacepark926@gmail.com](mailto:jacepark926@gmail.com) |
| **Contact:** | | Heung Youl Youm Chairman of JCA-DCC Korea (Republic of) | | | Tel: +82-41-530-1328 E-mail: [hyyoum@sch.ac.kr](mailto:hyyoum@sch.ac.kr) |

**Summary**

This document is to provide an update and ongoing maintenance of the Digital Covid Certificates (DCC) standards roadmap from ITU-T study groups and other groups, which have activities or documents related to digital COVID-19 certificates. This document is intended to be reviewed at the 3rd JCA-DCC meeting on 2 December 2022.

Annex A: DCC standards roadmap

**Annex A**

**DCC standards roadmap**

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

# Key international and regional DCC standards development and deployment activities (including approved standards and work items under development)

## Ecma International

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TC** | **Deliverable / Title** | **Scope / Abstract** | **Type** | **Status** | **Publication date** |
| [TC51](https://www.ecma-international.org/technical-committees/tc51/) | [Ecma-412 (ISO/IEC 20933), Framework for distributed real-time access systems](https://www.ecma-international.org/wp-content/uploads/ECMA-412_2nd_edition_june_2017.pdf) | This Standard specifies a framework for a distributed real-time access system. It includes:  1) an ID triggered modular system architecture, the functions of the modules, the semantics of messages those modules exchange, and elements of messages;  2) the system behaviour from the time it receives an access request until the time it sends the result along with the sequence;  3) performance measurement mechanisms using a time stamping function that can be employed for the evaluation of the system. | Standard | Published | 2017-06 |
| [TC51](https://www.ecma-international.org/technical-committees/tc51/) | [Ecma-417 (ISO/IEC 24643:2021), Architecture for a distributed real-time access system](https://www.ecma-international.org/wp-content/uploads/ECMA-417_3rd_edition_august_2021.pdf) | This Standard specifies the architecture for a distributed real-time access system. The architecture specifies the function group concept of the system, functionalities of each function group, and interfaces. Communication between function group and functions are not in the scope of this Standard. | Standard | Published | 2021-08-09 |

## ETSI

| **TC** | **Deliverable / Title** | **Scope / Abstract** | **Type** | **Status** | **Publication date** |
| --- | --- | --- | --- | --- | --- |
| [eHealth](https://www.etsi.org/committee/1396-ehealth) | [ETSI GS E4P 006 V1.1.1 (2021-05)](https://www.etsi.org/deliver/etsi_gs/E4P/001_099/007/01.01.01_60/gs_E4P007v010101p.pdf)  Europe for Privacy-Preserving Pandemic Protection (E4P); Device-Based Mechanisms for pandemic contact tracing systems | This document specifies various Proximity Detection Methods for Pandemic contact tracing systems, including proximity detection mechanisms of contacts, anonymous identification of contacts, storage requirements for proximity data of contacts. Methods are clarified in sufficient technical detail such that means of interoperability can be readily defined in a later Work Item. Each method is characterized (e.g. in a table) by its degree of compatibility with the E4P requirements work item. The initial version of this document may be revised several times as additional methods are added, e.g. including methods which are gaining consensus in non-European countries. | Group Specification | Published | 2021-05 |
| [eHealth](https://www.etsi.org/committee/1396-ehealth) | [ETSI GS E4P 007 V1.1.1 (2021-05)](https://www.etsi.org/deliver/etsi_gs/E4P/001_099/007/01.01.01_60/gs_E4P007v010101p.pdf)  Europe for Privacy-Preserving Pandemic Protection (E4P); Pandemic proximity tracing systems: Interoperability Framework | This document defines an interoperability framework for pandemic contact tracing systems which allows the centralized and decentralized modes of operation to fully interoperate. This document is part of the family of ISG E4P GS/GRs and thus aligned with GS “Requirements for Pandemic Contact Tracing Systems using Mobile Devices”. It covers interoperability between ROBERT, NHSX, DP3T, DESIRE, ProntoC2 and other applications/protocols as well as the different device platforms, some of which may emerge also during ISG E4P work. | Group Specification | Published | 2021-05 |
| [eHealth](https://www.etsi.org/committee/1396-ehealth) | [ETSI GS E4P 008 V1.1.1 (2021-05)](https://www.etsi.org/deliver/etsi_gs/E4P/001_099/008/01.01.01_60/gs_E4P008v010101p.pdf)  Europe for Privacy-Preserving Pandemic Protection (E4P); Back-End mechanisms for pandemic contact tracing systems | This document specifies back-end mechanisms for Pandemic contact Tracing Systems, including architecture, information flow, protocols for sharing proximity data of contacts, data protection, user privacy, information security and the requisite APIs (Application Programming Interfaces). Sufficient technical detail will be included to also facilitate means of interoperability in a later Work Item. Each system is characterized (e.g. in a table) by its degree of compatibility with the E4P requirements work item. The initial version of this document may be revised several times as additional methods are added, e.g. including methods which are gaining consensus in non-European countries. | Group Specification | Published | 2021-05 |
| [eHealth](https://www.etsi.org/committee/1396-ehealth) | [ETSI GR E4P 002 V1.1.1 (2021-02)](https://standards.iteh.ai/catalog/standards/etsi/46ad4bea-cb75-4a9d-bba1-87e86c64fe43/etsi-gr-e4p-002-v1-1-1-2021-02)  Europe for Privacy-Preserving Pandemic Protection (E4P); Comparison of existing pandemic contact tracing systems | This document provides a review of existing pandemic proximity detection methods, applications and other aspects of a pandemic contact tracing system. The similarities and differences of the various available or upcoming approaches are examined, particularly concerning but not limited to the degree of interoperability, security aspects, use of centralized or decentralized approach, use of particular proximity detection methods and technologies, support of different device platforms, epidemiological value and privacy aspects. The analysis also includes a grouping of various approaches into several similar types (e.g. centralized or decentralized system) and provides examples of use cases to which the approaches apply. The analysis is neutral in terms of technologies and use cases, however the focus is on cases involving proximity sensing and networking using mobile devices, and the applications and other technical enablers which can be installed on the devices. This document provides a basis for the analysis of suitable requirements for a tandardizat solution in Work Item D/E4P-003. | Group Report | Published | 2021-02 |
| [eHealth](https://www.etsi.org/committee/1396-ehealth) | [ETSI GS E4P 003 V1.1.1 (2021-04)](https://cdn.standards.iteh.ai/samples/59490/23ba4477c6ac4d71ba3f924718f54907/ETSI-GS-E4P-003-V1-1-1-2021-04-.pdf)  Europe for Privacy-Preserving Pandemic Protection (E4P); High level requirements for pandemic contact tracing systems using mobile devices | This document specifies the requirements for Pandemic Contact Tracing Systems using mobile devices. The use cases are defined addressing the key aspects of the system (reliability, accuracy, timeliness, privacy, security etc.) and reflecting the conclusions of GR “Comparison of existing pandemic contact tracing systems”. The relevant EU guidelines/requirements and a balance of trade-offs are considered, with the aim of achieving systems which are practical to deploy, will be used by the majority of users voluntarily, are compliant with the applicable laws and regulations, and provide seamless continuity of pandemic contact tracing for people travelling between countries. | Group Specification | Published | 2021-04 |
| [eHealth](https://www.etsi.org/committee/1396-ehealth) | [ETSI SR 003 809 V1.1.2 (2021-12)](https://www.etsi.org/deliver/etsi_sr/003100_003199/003186/01.01.01_60/sr_003186v010101p.pdf)  eHEALTH; The role of ICT to enable Health crisis management and recovery; Responding to the 2019 SARS-CoV-2 Pandemic | To provide a detailed review of actions to be taken by ETSI, in partnership with other SDOs and industrial development groups, in driving ICT standards to support societal responses to health crisis. The report shall consider the role played by ICT in response to the SARS-CoV-19 pandemic and shall identify where there were successes, where there were failures, and where ICT and particularly standards in ICT, may play a role in future mitigations. | Special Report | Published | 2013-12 |
| [eHealth](https://www.etsi.org/committee/1396-ehealth) | [ETSI TS 103 757 V2.1.1 (2021-08)](https://www.etsi.org/deliver/etsi_ts/103700_103799/103757/02.01.01_60/ts_103757v020101p.pdf)  SmartM2M; Asynchronous Contact Tracing System; Fighting pandemic disease with Internet of Things (IoT) | Asynchronous Contact Tracing (ACT) traces the IoT connected object that may have been infected by the Covid-19 virus (or future pandemic viruses).  This shifts the paradigm, from searching for a person in the process of infecting another to the tracing of both potential contamination and infections, and leveraging on the combination of the two information.  The scope of this WI is to standardize the full support of Asynchronous Contact Tracing (ACT) by means of  1) providing some examples of use and deployment of ACT by means of a few explanatory use cases.  2) specifying the ACT method and its interaction with deployed contact tracing applications for human and systems. This includes the interaction with the different technologies used by non ACT contact tracing solutions.  3) specifying the ACT system including application protocols and API.  The new ACT method will require the use of existing ready-to-market IoT-based technology and well-established wireless network techniques, in particular the ones specified in the ETSI standards ecosystem.  Moreover, it will preserve the user’s privacy in accordance with GDPR and/or other regional requirements not requiring the transmission of any personal information by the user. | Technical Specification | Published | 2021-08 |
| [eHealth](https://www.etsi.org/committee/1396-ehealth) | [DTR/eHEALTH-0015(TR 103 817)](https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=63029)  eHEALTH; Presence preserving proximity function trigger (3PFT) | The goal is the design of a multi-input privacy protected presence aware function triggering framework for use on smartphones and other IoT-devices for a variety of eHealth uses whilst the visitor is present at the venue.  Currently envisaged scenarios:-  - Visitors recording visits to host locations on their phones (venue check-in / check-out) either automatically (E.g. Bluetooth) or via scanning a QR code  - Venue recording of visitors with permission from the visitor  - Exposing venue services to visitors (E.g. internal navigation)  - Triggering of functions based on location making authorized use of the presence awareness within the restrictions agreed by visitors and hosts  - Recording of population density within a venue  - Tracking of venue-owned equipment  - Venue provided messaging system (E.g. replacement for hospital pagers)  - Alerting to a change in the position of equipment/visitors (geo-fencing). E.g. care home residents wandering off site  A wide variety of input for location-awareness will be possible, but in particular Bluetooth (LE and/or MESH) beacons and beacon like devices (including wearables), and optical QR code recognition will be supported.  This work item shall produce:-  - Recommendation for a venue check-in/out standard based on Bluetooth Low Energy that is compatible with manual QR code systems, and works in a single venue diary app  - Extension of the above to provide the device itself with an accurate position within the venue  - Extension of the above to specify how relevant venue diary segments are uploaded to a PHA for DCT with permission of the device user, sent to other devices, and interpreted by those devices, in a privacy preserving way  - Recommendation of a privacy preserving method and standard for discovering venue based services  - Recommendation of a mechanism to use a network of Bluetooth MESH beacons linked to venue server’s providing services  - Recommendation of a mechanism to provide future add-on services in a way that supports multiple vendors and providers of compatible equipment  Out of scope of this work:-  - Mandatory exchange of tokens from individuals’ devices (i.e. E4P exposure tokens of phones/wearables) in order to access venue services  - IP based IoT sensor networks  - WiFi / SSID detection or logging  - Detection of the presence of pathogens  - Asynchronous presence recording or alerting of physical items (i.e. things other than persons) | Technical Report | Early draft | 2022-12-23 |
| [eHealth](https://www.etsi.org/committee/1396-ehealth) | [RTR/eHEALTH-0009v131(TR 103 477)](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=61321&curItemNr=70&totalNrItems=195&optDisplay=100000&qSORT=TB&qETSI_ALL=&SearchPage=TRUE&qINCLUDE_SUB_TB=&qINCLUDE_MOVED_ON=&qEND_CURRENT_STATUS_CODE=11+WI%3BM58&qSTOP_FLG=N&qKEYWORD_BOOLEAN=&qCLUSTER_BOOLEAN=&qCLUSTER=13&qFREQUENCIES_BOOLEAN=&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=&qREPORT_TYPE=)  eHEALTH; Standardization use cases for eHealth (eHealth use cases v1.3.1) | To present a number of typical use cases in the eHealth domain and from their analysis to identify gaps in standardization. The analysis should cover aspects of link connectivity, network interconnectivity, semantic and syntactic interoperability, security (risks and provisions), and the existence of standards to meet each aspect. Furthermore the analysis should clearly identify actors and their roles, for each of primary, secondary and tertiary involvement in the use case. Examples will be sought from industry, from existing and completed FP7 and H2020 projects and from current eHealth and Health industry practices. | Technical Report | Early draft | 2023-02-25 |
| [eHealth](https://www.etsi.org/committee/1396-ehealth) | [DES/eHEALTH-008 (ES 203 668)](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=56908&curItemNr=71&totalNrItems=181&optDisplay=100000&qSORT=TB&qETSI_ALL=&SearchPage=TRUE&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qEND_CURRENT_STATUS_CODE=11+WI%3BM58&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qCLUSTER_BOOLEAN=OR&qCLUSTER=13&qFREQUENCIES_BOOLEAN=OR&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=)  [eHEALTH Data recording requirements for eHealth](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=56908&curItemNr=71&totalNrItems=181&optDisplay=100000&qSORT=TB&qETSI_ALL=&SearchPage=TRUE&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qEND_CURRENT_STATUS_CODE=11+WI%3BM58&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qCLUSTER_BOOLEAN=OR&qCLUSTER=13&qFREQUENCIES_BOOLEAN=OR&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=) | The aim of this work is to identify the requirements for recording eHealth events, i.e. those from ICT based eHealth devices and from health practitioners. On the understanding, illustrated in the use case document and in the White Paper, that health records are subject to security and privacy constraints, but at the same time need to be available to many different stakeholders across time and space without pre-cognition of who those stakeholders are. The purpose of this technical specification is to very carefully specify at stage1 and stage 2 level the normative framework for ensuring events/transactions related to a patient are recorded accurately by identifiable entities (devices or health professionals) and made available with minimum delay to any other health professional (i.e. to ensure that actions taken by one health professional is visible to any other health professional irrespective of location without delay). The normative framework is intended to be adopted by all groups contributing to eHealth including CYBER, smartM2M, smartBAN. Close cooperation should be maintained within ETSI (as above) and also with external partners including the EuroRec Institute and IEEE. | Standard | Early draft | 2023-02-11 |

## European Commission

The following technical specifications published as Guidelines provide further explanations and instructions complementing the adopted European Commission Implementing Decisions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Deliverable / Title** | **Scope / Abstract** | **Status** | **Publication date** |
| [Commission Implementing Decision (EU) 2021/1073 Of 28 June 2021](https://op.europa.eu/en/publication-detail/-/publication/ec12b5be-d967-11eb-895a-01aa75ed71a1#:~:text=Home-,Commission%20Implementing%20Decision%20(EU)%202021%2F1073%20of%2028%20June,Council%20(Text%20with%20EEA%20relevance)) | Laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate established by Regulation (EU) 2021/953 of the European Parliament and of the Council | Published | 2022-04-25 |
| [Guidelines on Value Sets for EU Digital COVID Certificates](https://ec.europa.eu/health/document/download/3df9e6fd-a616-4727-a374-fcdbee0883fd_en) Volume 1 | Value Sets for the EU Digital COVID Certificate are defined for the datasets provided in the Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic. | Published | 2022-10-06 |
| [Technical Specifications for EU Digital COVID Certificates](https://health.ec.europa.eu/document/download/c58ae062-06a8-41e1-815e-9bb820baeab9_en?filename=digital-covid-certificates_v1_en.pdf) Volume 1 | This document specifies a generic data structure and encoding mechanisms for electronic health certificates. It also specifies a transport encoding mechanism in a machine‐readable optical format (QR), which can be displayed on the screen of a mobile device or printed on a piece of paper | Published | 2022-02-23 |
| [Technical Specifications for EU Digital COVID Certificates Volume 3 Interoperable 2D Code](https://health.ec.europa.eu/document/download/73b2078f-2a52-48a1-abf5-d5788c3d3af6_en?filename=digital-covid-certificates_v3_en_0.pdf) | Annex I of the Commission Implementing Decision (EU) 2021/1073 of 28 June 2021 describes general rules for interoperable 2D codes. | Published | 2022-02-23 |
| [Technical Specifications for EU Digital COVID Certificate Applications Version 1.5](https://health.ec.europa.eu/document/download/c0a07892-a01c-4bc8-8e9f-1e91d9597d17_en?filename=digital-covid-certificates_v4_en.pdf) | This document describes the issuer app, wallet app, verifier app, and core functionalities of the required national certificate backends as required by EU-wide DCC verification. | Published | 2022-06-15 |
| [Public Key Certificate Governance](https://ec.europa.eu/health/document/download/79556061-92df-40e1-92af-c054847d76ab_en) | Annex IV of the Commission Implementing Decision (EU) 2021/1073 of 28 June 2021 describes general rules for the public key certificate governance. | Published | 2022-02-23 |
| [Technical Specifications for EU Digital COVID Certificates Validation Rules](https://health.ec.europa.eu/document/download/b3833231-ebd7-4dad-871b-6a962b9b3c2d_en?filename=eu-dcc_validation-rules_en.pdf) | The EU DCC Validation Rules are applied on the payload of the DCC. All “technical" validations have to be performed in the verifier applications to ensure that these checks are not overridden. | Published | 2022-02-23 |
| [Validation of EU Digital COVID Certificates in the context of air transport](https://health.ec.europa.eu/document/download/08177755-5d73-448b-8a18-d38590d0da2c_en?filename=covid-certificate_air-transport_en.pdf) | This document is providing different scenarios and solutions to check EU DCCs in the setting of a passenger journey in air transportation. It is intended to facilitate discussion and provide different possible solutions for airlines and Member States. However, the document does not provide guidance on how passenger can fully comply with various health measures or travel history that Member States may require for entry. | Published | 2021-06-30 |
| [Guidelines on the use of Digital Covid Certificates in traveller and online booking scenarios](https://health.ec.europa.eu/document/download/3c25f72e-5142-41d5-a283-577d68460e62_en?filename=covid-certificate_traveller-onlinebooking_en.pdf) | This document specifies the Digital Covid Certificate (DCC) features applicable to traveller & online booking scenarios (Version 1.2). It provides specifications for the support functions and services applicable to travel booking/check-in scenarios as well as some additional features enhancing the EU DCC digital wallet. DCC Gateway core functionalities and central interfaces remain untouched. | Published | 2021-10-20 |
| [DCC Anomaly Capture Process for COVID Certificate Data](https://health.ec.europa.eu/document/download/3bf8bc90-5093-441a-a4d1-25543e3aa184_en?filename=covid-certificate_dcc_anomaly-capture-process_en.pdf) | This document sets out a process for the privacy preserving handling of the invitro scans. The GDPR and other legal considerations are out of scope; nor does this document make any assumption about which party should be responsible for the (initial) scan or the data. Any processing of personal data must comply with GDPR. | Published | 2021-09-15 |
| [Guidelines on Paper version of the EU Digital COVID Certificate](https://health.ec.europa.eu/document/download/ea2e350c-0992-4993-98b1-f752647cb179_en?filename=covid-certificate_paper_guidelines_en.pdf) | - | Published | 2021-05-26 |
| [Guidelines on EU DCC Revocation - B2A Communication between the Backend and the Applications Version 1.1](https://ec.europa.eu/health/document/download/52236abb-5039-475e-aa1a-9c75ea7adda9_en) | This document is a guideline on how to download and process the revocation list data1 from the EU DCC Gateway (DCCG) and use it within the associated wallet / verifier apps and validation services. It complements the DCC Revocation B2B concept, which describes the DCCG interfaces / access points for revocation of single DCCs. | Published | 2022-03-30 |

## ICAO

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Deliverable / Title** | **Scope / Abstract** | **Type** | **Status** | **Publication date** |
| [Implementing a Visible Digital Seal for Non-Constrained Environments (VDS-NC) for Travel-Related Health Proofs](https://www.icao.int/secretariat/TechnicalCooperation/Pages/VDS-NC-iPACK.aspx) | This Implementation Package (iPack) is a self-contained package aimed at assisting and guiding State authorities such as ministries of interior, foreign affairs, health and technology, and their agencies, in the implementation of the ICAO Visible Digital Seal for Non-Constrained Environments (VDS-NC) as a secure tool for encoding health information for use in travel.  It includes relevant documentation, tools and a virtual course to build capacities for the implementation of all technical, organizational and administrative arrangements necessary for the issuing of health proofs containing VDS-NC barcodes that will be read and trusted globally and for the proper validation of the health proofs issued by others. A dedicated expert will work remotely with the designated stakeholders, providing guidance in their implementation efforts to achieve the objectives of the iPack. The level of progress made in achieving each iPack objective depends on the availability of States’ resources to perform the work. | Technical Report | Published | 2021-04-23 |

## ISO

| **TC** | **Deliverable / Title** | **Scope / Abstract** | **Type** | **Status** | **Publication date** |
| --- | --- | --- | --- | --- | --- |
| [TC 215](https://www.iso.org/committee/54960.html) | [ISO 17090-1:2021, Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services](https://www.iso.org/standard/81430.html) | This document defines the basic concepts underlying the use of digital certificates in healthcare and provides a scheme of interoperability requirements to establish a digital certificate-enabled secure communication of health information. It also identifies the major stakeholders who are communicating health-related information, as well as the main security services required for health communication where digital certificates can be required.  This document gives a brief introduction to public key cryptography and the basic components needed to deploy digital certificates in healthcare. It further introduces different types of digital certificates — identity certificates and associated attribute certificates for relying parties, self-signed certification authority (CA) certificates, and CA hierarchies and bridging structures. | International Standard | Published | 2021-03 |
| [TC 215](https://www.iso.org/committee/54960.html) | [ISO 17090-2:2015](https://www.iso.org/standard/63020.html?browse=tc), Health informatics — Public key infrastructure — Part 2: Certificate profile | ISO 17090-2:2015 specifies the certificate profiles required to interchange healthcare information within a single organization, between different organizations and across jurisdictional boundaries. It details the use made of digital certificates in the health industry and focuses, in particular, on specific healthcare issues relating to certificate profiles. | International Standard | Published | 2015-11 |
| [TC 215](https://www.iso.org/committee/54960.html) | [ISO 17090-3:2021](https://www.iso.org/standard/81431.html?browse=tc), Health informatics — Public key infrastructure — Part 3: Policy management of certification authority | This document gives guidelines for certificate management issues involved in deploying digital certificates in healthcare. It specifies a structure and minimum requirements for certificate policies, as well as a structure for associated certification practice statements.  This document also identifies the principles needed in a healthcare security policy for cross-border communication and defines the minimum levels of security required, concentrating on aspects unique to healthcare. | International Standard | Published | 2021-03 |
| [TC 215](https://www.iso.org/committee/54960.html) | [ISO 17090-4:2020](https://www.iso.org/standard/74357.html?browse=tc), Health informatics — Public key infrastructure — Part 4: Digital signatures for healthcare documents | This document supports interchangeability of digital signatures and the prevention of incorrect or illegal digital signatures by providing minimum requirements and formats for generating and verifying digital signatures and related certificates.  This document describes the common technical, operational, and policy requirements that need to be addressed to enable digital certificates to be used in protecting the exchange of healthcare information within a single domain, between domains, and across jurisdictional boundaries. Its purpose is to create a platform for global interoperability. It specifically supports digital certificate enabled communication across borders but could also provide guidance for the national or regional deployment of digital certificates in healthcare.  It defines the provable compliance with a PKI policy necessary in the domain of healthcare. This document specifies a method of adopting long-term signature formats to ensure integrity and non-repudiation in long-term electronic preservation of healthcare information.  This document provides Healthcare specific PKI (HPKI) profiles of digital signature based on the ETSI Standard and the profile of the ISO/ETSI Standard specified in CAdES, XAdES, and PAdES. | International Standard | Published | 2020-10 |
| [TC 215](https://www.iso.org/committee/54960.html) | [ISO 17090-5:2017](https://www.iso.org/standard/67883.html?browse=tc), Health informatics — Public key infrastructure — Part 5: Authentication using Healthcare PKI credentials | ISO 17090-5:2017 defines the procedural requirements for validating an entity credential based on Healthcare PKI defined in the ISO 17090 series used in healthcare information systems including accessing remote systems. Authorization procedures and protocols are out of scope of this document. The data format of digital signatures is also out of scope of this document. | International Standard | Published | 2017-07 |
| [TC 215](https://www.iso.org/committee/54960.html) | [ISO 27799:2016 Health informatics — Information security management in health using ISO/IEC 27002](https://www.iso.org/standard/62777.html) | ISO 27799:2016 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).  It defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that International Standard. | International Standard | Published | 2016-07 |

## ISO/IEC JTC 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SC** | **Deliverable / Title** | **Scope / Abstract** | **Type** | **Status** | **Publication date** |
| [SC 17](https://www.iso.org/committee/45144.html) | [Visible Digital Seal for non-constrained environments](https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Visible%20Digital%20Seal%20for%20non-constrained%20environments.pdf) | The VDS-NC is a general definition and can be used for any situation where the size of the barcode is not a serious constraint. The specification details the structure, the trust framework and the signature component. Two health related use cases are also described in this TR. Further use cases will be added to this TR as the necessity arises. | Technical Report | Published | 2021-04-23 |
| [SC 17](https://www.iso.org/committee/45144.html) | [ISO/IEC 18013-5:2021, Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application](https://www.iso.org/standard/69084.html) | This document establishes interface specifications for the implementation of a driving licence in association with a mobile device. This document specifies the interface between the mDL and mDL reader and the interface between the mDL reader and the issuing authority infrastructure. This document also enables parties other than the issuing authority (e.g. other issuing authorities, or mDL verifiers in other countries) to:  — use a machine to obtain the mDL data;  — tie the mDL to the mDL holder;  — authenticate the origin of the mDL data;  — verify the integrity of the mDL data.  The following items are out of scope for this document:  — how mDL holder consent to share data is obtained;  — requirements on storage of mDL data and mDL private keys. | International Standard | Published | 2021-09 |
| [SC 31](https://www.iso.org/committee/45332.html) | [ISO/IEC 18004: 2015, Automatic identification and data capture techniques — QR Code bar code symbology specification](https://www.iso.org/standard/62021.html) | ISO/IEC 18004:2015 defines the requirements for the symbology known as QR Code. It specifies the QR Code symbology characteristics, data character encoding methods, symbol formats, dimensional characteristics, error correction rules, reference decoding algorithm, production quality requirements, and user-selectable application parameters. | International Standard | Published | 2015-02 |
| [SC 31](https://www.iso.org/committee/45332.html) | [ISO/IEC 23941:2022, Information technology — Automatic identification and data capture techniques — Rectangular Micro QR Code (rMQR) bar code symbology specification](https://www.iso.org/standard/77404.html) | This document defines the requirements for the symbology known as rMQR. It specifies the rMQR symbology characteristics, data character encoding methods, symbol formats, dimensional characteristics, error correction rules, reference decoding algorithm, printing quality requirements and user-selectable application parameters. | International Standard | Published | 2022-05 |

## ITU-T

| **SG/FG** | **Deliverable / Title** | **Scope / Abstract** | **Type** | **Status** | **Target date** |
| --- | --- | --- | --- | --- | --- |
| [SG17](https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx) | [ITU-T X.Sup38](https://www.itu.int/rec/T-REC-X.Sup38/en) ITU-T X.1152 - Supplement on use cases for contact tracing technologies to prevent spread of infectious diseases | Supplement 38 to Recommendation ITU-T X.1152 defines a contact tracing application as a tool that enables the identification, assessment, and management of people who have been in contact with individuals that may have been infected with a contagious disease to prevent onward transmission. These applications help prevent the spread of infectious diseases by proactively finding people at higher risk than others due to potential exposure, notifying them if possible, and quarantining them if necessary. This Supplement guides the development of interoperable systems to automatically trace and inform potentially infected users, in addition to manual notification methods, with consideration for reducing potential security risks associated with data processed in contact tracing applications. It also describes various use cases for contact tracing applications, provides data processing models including their data processing flow and identifies threats and risks from a security and PII protection perspective. | Supplement | Agreed | 2022-09 |
| [SG17](https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx) | [ITU-T X.suppl.uc-dcc](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18350) Supplement to X.1152 - Use cases for digital COVID-19 certificates | The Digital COVID-19 Certificate is to provide proof that a person has been vaccinated against COVID-19, tested for the virus, or recovered from COVID-19. Current COVID-19 pandemic has illustrated the urgent need for digital COVID-19 certificates including vaccination etc. that could be used in an interoperable fashion across organizations. WHO (World Health Organization) recently published the WHO Technical Specifications and Implementation Guidance on digital Documentation of COVID-19 Certificates: Vaccination Status (DDCC:VS). Public key infrastructure (PKI) governs the issuance of digital certificates to protect sensitive data, provide unique digital identities for users, devices and applications and secure end-to-end communications. Decentralized identity is an emerging concept that gives back control of identity to consumers using an identity wallet in which they collect verified information about themselves from certified issuers. The digital COVID-19 certificates should be designed using both existing technology such as QR code and public key infrastructure (PKI) and emerging technologies such as decentralized identity (DID). This Supplement identifies use cases for implementing digital COVID-19 certificates. It provides digital COVID-19 certificates based on public key infrastructure as well as those based on decentralized identity. It also describes the common data format for digital COVID-19 certificate and scenarios for establishing trust network for digital COVID-19 certificates. | Supplement | Under development | 2024-03 |
| [SG17](https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx) | [ITU-T X.gpwd](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18011) Threat Analysis and guidelines for securing password and password-less authentication solutions | This Recommendation performs security and threat analysis of authentication solutions that are based on some form of a shared secret. The work takes a close look into security risks associated with password systems and emerging password-less solutions. The Recommendation performs threat analysis and develops guidelines and best practices for the protection of users and accounts based on these methods. This work represents a bridge to be used for those adopters that need to support legacy solutions as they do migrate to stronger authentication methods such as FIDO (X.1277 and X.1278). | Recommendation | Under development | 2023-09 |
| [SG17](https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx) | [ITU-T X.dpki](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18505) Decentralized Public-key Infrastructure | The scope of this Recommendation | International Standard is to provide a scalable specification for a widely distributed public-key infrastructure (PKI) with a decentralized approach based on the blockchain technology resulting in a specification for a decentralized public-key infrastructure (DPKI). DPKI allows a world-wide federated PKI, where trust is established by consensus rather than relying on trust anchors and long chain of trusts.  As the DPKI is blockchain based, each node in the network holds a replica of the decentralized ledger with all the included transactions. In addition, each node has a replica of a director, called the state directory, where the updated state of the DPKI information is maintained. This information includes information about CAs and their submitted DPKI version of public-key certificates called DPKI certificates.  Relying parties may get rapid response on the status of any DPKI certificate generated anywhere in the world. | Recommendation | Under development | 2024 |
| [SG17](https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx) | [ITU-T X.1250rev Baseline capabilities for enhanced global identity management and interoperability](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18005) | Recommendation ITU-T X.1250 describes baseline capabilities for global identity management (IdM) interoperability (i.e., to enhance exchange and trust in the identifiers used by entities in telecommunication/information technology IT networks and services). The definitions and need for IdM are highly context-dependent and often subject to very different policies and practices in different countries. The capabilities include the protection and control of personally identifiable information (PII). | Recommendation | Under development | 2023-09 |
| [SG17](https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx) | [ITU-T X.1251rev A framework for user control of digital identity](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18027) | This Recommendation defines a framework to enhance user control and exchange of their digital identity related information.  This Recommendation also defines capabilities for the digital identity information exchange. The work includes providing the user with the ability to control the release of personally identifiable information.  This Recommendation will focus on the use of emerging of decentralized identity protocols for exchanging verifiable user credentials. In particular, digital wallets will be considered as the main mechanisms for user control of their identity data. | Recommendation | Under development | 2023-09 |
| [SG17](https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx) | [ITU-T X.srdidm Security requirements for decentralized identity management systems using distributed ledger technology](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18037) | This Recommendation describes security requirements for decentralized identity management systems using distributed ledger technology (DLT). It focuses on defining decentralized identity management models using DLT and assurance levels. And it also focuses on identifying security threats to decentralized identity management systems using DLT, specifying security requirements against the identified security threats, and providing use cases. | Recommendation | Under development | 2024-09 |
| [SG20](https://www.itu.int/en/ITU-T/studygroups/2022-2024/20/Pages/default.aspx) | [ITU-T Y.FSPH Framework for smart public health emergency management in smart and sustainable cities](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18460) | This Recommendation specifies the framework of smart public health management in Smart and Sustainable Cities (SSC). The motivation for its development is based on the fact that the world experienced a coronavirus pandemic lately, which has impacted all avenues of life, especially in cities with growing populations which have proved to be more vulnerable to such crises. | Recommendation | Under development | 2023 |
| [SG20](https://www.itu.int/en/ITU-T/studygroups/2022-2024/20/Pages/default.aspx) | [ITU-T Y.RA-PHE](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17921) Requirements and reference architecture of smart service for public health emergency | This new draft Recommendation identifies requirements of smart service for public health emergency and corresponding management and specifies a reference architecture of smart service for public health emergency. The scope of this draft new Recommendation includes: - Introduction of smart service for public health emergency and for public health emergency management; - Requirements of smart service for public health emergency and for its ICT implementations; - Reference architecture of smart service for public health emergency. | Recommendation | Under development | 2023-Q3 |
| [FG-AI4H](https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/default.aspx) | [FG AI4H DT4HE Output 1](https://www.itu.int/en/ITU-T/focusgroups/ai4h/Documents/FGAI4H-DT4HE-O-001.pdf)  Guidance on digital technologies for COVID health emergency | This deliverable collects effective ways and use cases demonstrating how AI and other digital technologies have combatted COVID-19 through the lifecycle stages of public health emergency management, including prevention, preparedness, response, and recovery. The outputs are expected to evolve towards a more generalizable mechanism on the health emergency continuum, eventually applicable to other pandemics. | Technical Report | Published | 2020-11-30 |

## WHO

|  |  |  |  |
| --- | --- | --- | --- |
| **Deliverable / Title** | **Scope / Abstract** | **Status** | **Publication date** |
| [Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance](https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1) | This is a guidance document for countries and implementing partners on the technical requirements for developing digital information systems for issuing standards-based interoperable digital certificates for COVID-19 vaccination status, and considerations for implementation of such systems, for the purposes of continuity of care, and proof of vaccination. | Published | 2021-08-27 |
| [Digital documentation of COVID-19 certificates: vaccination status: web annex A: DDCC:VS core data dictionary, 27 August 2021](https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-Digital_certificates-vaccination-data_dictionary-2021.1) | This is a guidance document for countries and implementing partners on the technical requirements for developing digital information systems for issuing standards-based interoperable digital certificates for COVID-19 vaccination status, and considerations for implementation of such systems, for the purposes of continuity of care, and proof of vaccination. | Published | 2021-08-27 |
| [Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance, web annex B: technical briefing,](https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-Digital_certificates-vaccination-technical_briefing-2021.1) | This is a guidance document for countries and implementing partners on the technical requirements for developing digital information systems for issuing standards-based interoperable digital certificates for COVID-19 vaccination status, and considerations for implementation of such systems, for the purposes of continuity of care, and proof of vaccination. | Published | 2021-08-27 |
| [Global Trust Network: Part 1: Trust List Specification](https://github.com/WorldHealthOrganization/ddcc-trust/blob/main/TrustListSpecification.md) | As part of the WHO DDCC effort, we are striving to architect a Global Trust Network that can bring existing and new local and regional trust networks together in a way that respects their designs and sovereignty while contributing to real interoperability among all of them.  Note: This is a working document drafted by the WHO service team to kick off technical discussions on the Trust List Specification for a Global Trust Network. Everything discussed in this document is work in progress and none of the things is set in stone. | Under development | - |

# Gap analysis on DCC standard development activities

To be provided, call for contributions is issued from the editors to JCA-DCC members

# Approved DCC standards

To be provided, call for contributions is issued from the editors to JCA-DCC members

# Best practices

To be provided, call for contributions is issued from the editors to JCA-DCC members

# Other relevant DCC activities and papers

To be provided, call for contributions is issued from the editors to JCA-DCC members

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