

Supplement

ITU-T X Suppl. 40 (03/2024)

SERIES X: Data networks, open system communications
and security

Supplements to ITU-T X-series Recommendations

ITU-T X.1152 – Supplement on use cases for digital COVID-19 certificates

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METaverse AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

For further details, please refer to the list of ITU-T Recommendations.

Supplement 40 to ITU-T X-series Recommendations

ITU-T X.1152 – Supplement on use cases for digital COVID-19 certificates

Summary

Supplement 40 to Recommendation ITU-T X.1152 provides use cases for digital corona virus disease 2019 (COVID-19) certificates. It specifies digital COVID-19 certificates (DCCs) based on public key infrastructure (PKI) and those based on decentralized identity (DID). Supplement 40 to Recommendation ITU-T X.1152 also describes a common data format for DCCs and scenarios for establishing trust network supporting DCCs.

A DCC proves that a person has been vaccinated against COVID-19, tested for the virus or has recovered from COVID-19. The COVID-19 pandemic requires DCCs including details of vaccination that can be used in an interoperable fashion across organizations.

In 2021, the World Health Organization published *Digital documentation of COVID-19 certificates: Vaccination status: Technical specifications and implementation guidance*, which specifies PKI governing the issuance of digital certificates to: protect sensitive data; provide unique digital identities for users (holders), devices and applications; and secure end-to-end communications.

DCCs can be designed using such technologies as quick-response code, PKI and DID. DID is an emerging technology that gives back control of identity to users (verifiable credential holder) using an identity wallet in which they collect verified information about themselves from certified issuers.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X Suppl. 40	2024-03-01	17	11.1002/1000/15945

Keywords

Digital COVID-19 certificate, decentralized identity-based certificate, personally identifiable information (PII), public key infrastructure (PKI) based certificate.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the standards development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Supplement	1
4 Abbreviations and acronyms	2
5 Conventions	3
6 Overview	3
7 Types of COVID-19 certificate	3
8 Use cases for digital COVID-19 certificates	4
8.1 PKI-based digital COVID-19 certificates	4
8.2 Decentralized identity based digital COVID-19 certificates	5
9 Data format of digital COVID-19 certificates	6
9.1 Data elements used in WHO DCC	6
9.2 Data element in EU DCC	7
10 Establishing trust network for digital COVID-19 certificates	8
10.1 Trust network for PKI-based DCC	8
10.2 Trust network for DID-based DCC	10
Appendix I – Digital signature	11
Appendix II – Data protection principles for a DCC	12
Bibliography.....	13

Supplement 40 to ITU-T X-series Recommendations

ITU-T X.1152 – Supplement on use cases for digital COVID-19 certificates

1 Scope

This Supplement provides use cases for digital corona virus disease 2019 (COVID-19) certificates. It specifies digital COVID-19 certificates (DCCs) based on both public key infrastructure (PKI) and those based on decentralized identity (DID). It also describes a data format for DCCs and how trust networks can be established (such as a certificate chain of trust) supporting DCCs.

2 References

[ITU-T X.1152] Recommendation ITU-T X.1152 (2008), *Secure end-to-end data communication techniques using trusted third party services*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 certification authority (CA) [b-ITU-T X.509]: An authority trusted by one or more entities to create and digital sign public-key certificates. Optionally the certification authority may create the subjects' keys.

3.1.2 data controller [b-ITU-T X.1148]: Stakeholder (or privacy stakeholder) that determines the purposes and means for processing data other than natural persons who use data for personal purposes.

3.1.3 decentralized identity [b-ISO/IEC 22739]: Identity that is managed in a decentralized system.

3.1.4 decentralized system [b-ISO/IEC 22739]: Distributed system wherein control is distributed among the persons or organizations participating in the operation of the system.

Note – In a decentralized system, the distribution of control among persons or organizations participating in the system is determined by the system's design.

3.1.5 personally identifiable information (PII) [b-ISO/IEC 29100]: Information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person.

Note – The "natural person" in the definition is the PII principal. To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

3.1.6 public-key certificate [b-ITU-T X.509]: The public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority (CA) that issued it.

3.1.7 public-key infrastructure (PKI) [b-ITU-T X.509]: The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.

3.1.8 trust network [b-ISO/IEC 18013-3]: Component of a trust model that describes the trust relationships and chains between issuing authorities.

3.2 Terms defined in this Supplement

This Supplement defines the following terms: