X.509 usage in Global Health

ITU X.509 Day
9 May 2023

Dr. Carl Leitner, Technical Officer
Digital Health and Innovations Department, Science Division

World Health Organization

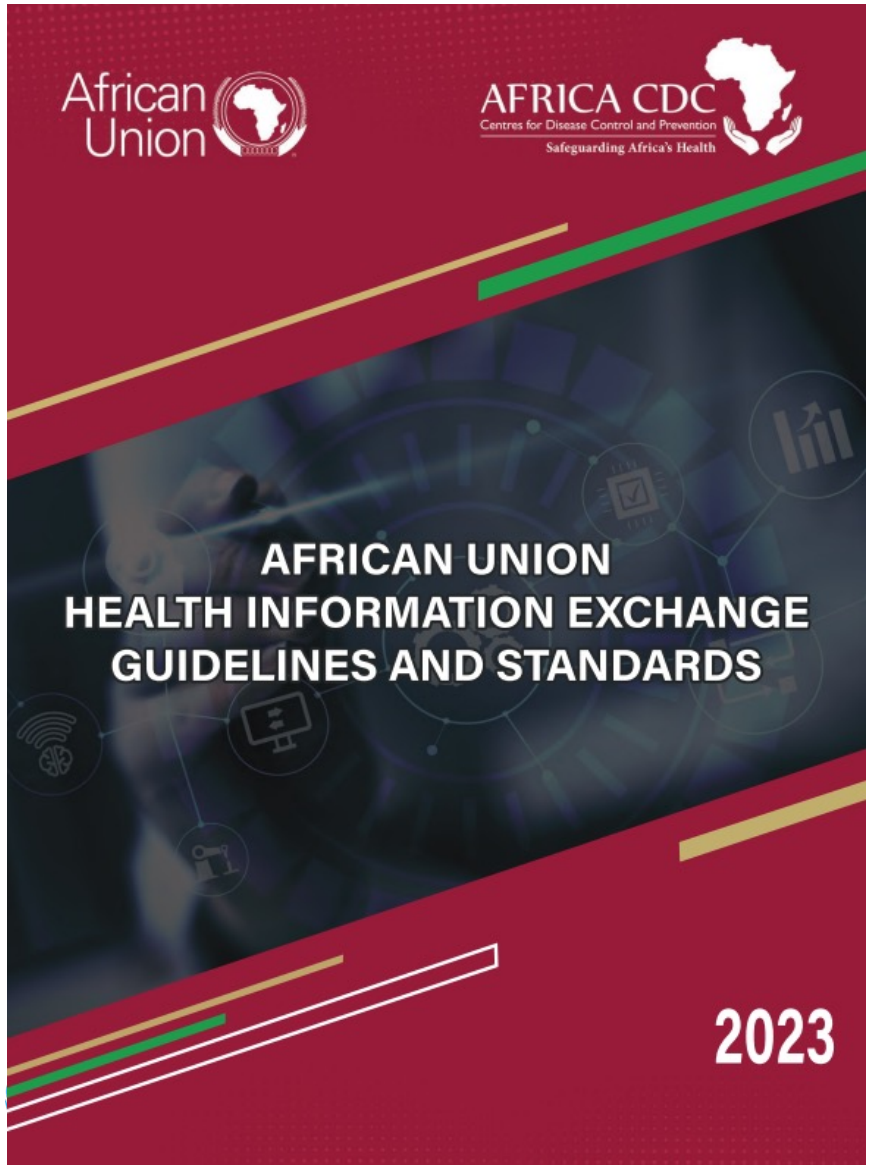
Global Strategy on Digital Health Policy Actions

Policy Action

Recommends defining “a national digital health architecture blueprint or road map, adopt **open-source health data standards** and aim for **reusable systems or assets** including interoperability of health information systems both at national and international levels in order to establish an innovative integration of **different digital technologies using shared services, ensuring data are of good and comparable quality**”

“Digital health should be an integral part of health priorities and benefit people in a way that is ethical, safe, secure, reliable, equitable and sustainable. It should be developed with principles of transparency, accessibility, scalability, replicability, interoperability, **privacy, security and confidentiality**.

African Union & Africa CDC: HIE Guidelines and Standards



Africa CDC recommends:

"Certificates: ITU-T X.509 digital certificates for use in public key encryption for TLS and S/MIME. To be used in conjunction with Public Key Cryptography Standards 7 (PKCS7) Cryptographic Message Syntax [IETF RFC 5652] and Public Key Cryptography Standards 12 (PKCS12) Personal Information Exchange Syntax Standard [IETF RFC 7292]. ● Hashing algorithms: NIST Secure Hashing Algorithm 2 (SHA-2) to include SHA”

Securing Communication Endpoints – Australia Example

AU Base Implementation Guide
4.1.1 - CI Build

Home | Guidance | FHIR Artefacts | Examples | Downloads | Change Log

Table of Contents > Artifacts Summary > Encryption Certificate PEM X509

AU Base Implementation Guide, published by HL7 Australia. This is not an authorized publication; it is the continuous build for version 4.1.1). This version is based on the current content of https://github.com/hl7au/au-fhir-base/ and changes regularly. See the Directory of published versions

Content | Detailed Descriptions | XML | JSON | TTL

9.76.1 Extension: Encryption Certificate PEM X509

Official URL: `http://hl7.org.au/fhir/StructureDefinition/encryption-certificate-pem-x509`		*Version*: **4.1.1**
Standards status: Trial-use	Maturity Level: 3	*Computable Name*: `EncryptionCertificatePEMx509`
Copyright/Legal: HL7 Australia© 2018+; Licensed Under Creative Commons No Rights Reserved.		

This extension applies to the Endpoint resource and is used to support encrypted certificate content for use with an endpoint. This extension allows an endpoint entry to define a suitable certificate for use in communications on the associated channel.

This extension may be used on the following element(s):

- Element ID Endpoint

9.76.1.1 Usage Notes

Profile specific implementation guidance:

- The value recorded is an X509 certificate in PEM format as per RFC7468.

Usage:

- Examples for this Extension: Telstra Health Secure Messaging Endpoint

Integrating the Health Enterprise (IHE) – Digital Signatures

IHE INTERNATIONAL | Integrating the Healthcare Enterprise

IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 19.0, June 17, 2022 – Final Text

Search | Search

HOME / ITI / TECHNICAL FRAMEWORK / VOLUME 1 / DOCUMENT DIGITAL SIGNATURE (DSG)

The Final Text ITI Technical Framework is published here in HTML format and is no longer published as PDF. Trial Implementation supplements are available from the Volume 1 Table of Contents.

37 Document Digital Signature (DSG)

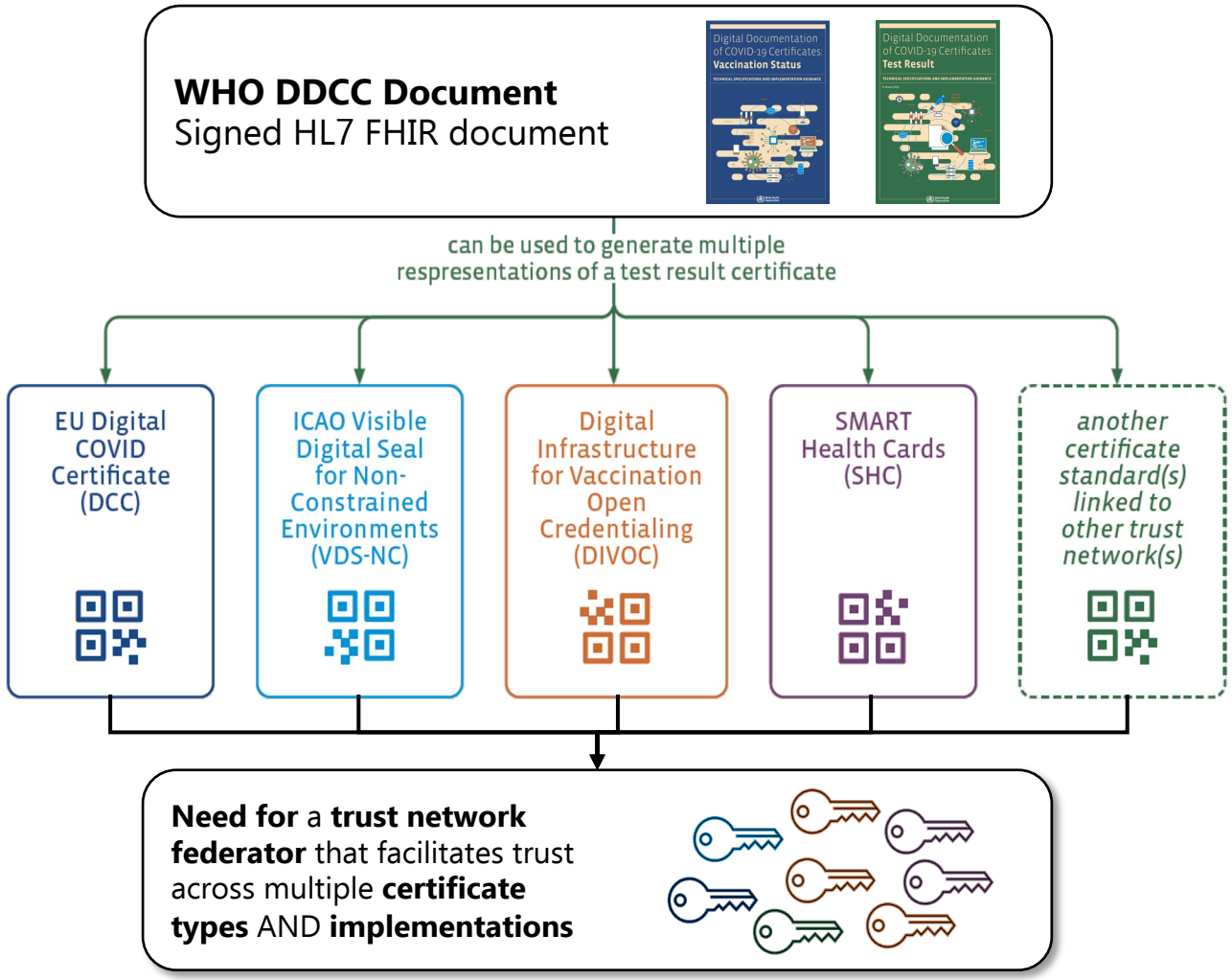
The Document Digital Signature (DSG) Profile defines general purpose methods of digitally signing of documents for communication and persistence. Among other uses, these methods can be used within an IHE Document Sharing infrastructure (e.g., XDS, XCA, XDM, XDR, and MHD). There are three methods of digital signature defined here: Enveloping, Detached (manifest), and SubmissionSet.

- An Enveloping Signature is a Digital Signature Document that contains both the signature block and the content that is signed. Access to the contained content is through removing the Enveloping - Digital Signature. Among other uses, this method should not be used with Document Sharing infrastructure.
- A Detached Signature is a Digital Signature Document that contains a manifest that points at independently managed content. Detached signatures leave the signed document or documents in the original form. Among other uses, this method is recommended for use with a Document Sharing infrastructure to support Digital Signatures, as this method does not modify the original Document Content. This method uses the Document Sharing “SIGNS” relationship provides linkage.
- A SubmissionSet Signature is a Detached Signature Document that attests to the content in a SubmissionSet by: containing a manifest of all the other Documents included in the SubmissionSet, and

- Document Digital Signature content shall conform to XAdES schema for signatures
- The PKI should adhere to ISO TS-17090 standards for PKI in healthcare

Global Digital Health Certification Network – COVID Certificates

World Health Organization



Computable components described in HL7 FHIR Implementation Guide as part of WHO SMART Guidelines

Multiple specifications for digitally signed QR codes using PKI

PKI Infrastructure in GDHCN Gateway:

- EU DCC API & certificate governance will be preserved
- DID for public key distribution supported

Decentralized PKI - LACChain

World Health Organization

LACCHAIN | eosio

Home LACChain EOSIO Tools Documentation

The EOSIO Blockchain Network for Latin America and the Caribbean

LACChain EOSIO enables organizations and developers to build blockchain applications on the LACChain network powered by EOSIO technology.

Thank you!

leitnerc@who.int