Healthcare Transformation with Informatics and Artificial Intelligence
J. Mantas et al. (Eds.)

doi:10.3233/SHTI230463

Patient-Centric Interoperability and Cybersecurity for Cross-Border Healthcare

Fernando LATORRE[a,b,c,1], Claudia E HAWKS[a], Bruno COLMENARES[a], Deepika VERMA[b], Marisa GIL[a,c] and Nuria SALA[a,b,c]
[a] *Conéctate Soluciones y Aplicaciones, S.L., Soria, CYL, Spain*
[b] *Connecting Solution and Applications, Ltd., Vancouver, BC, Canada*
[c] *Fundación UNID, Soria, CYL, Spain*
ORCiD ID: Fernando Latorre https://orcid.org/0009-0004-6313-6471, Claudia E Hawks https://orcid.org/0000-0002-2099-3543, Nuria Sala https://orcid.org/0009-0001-0556-0694

Abstract. In Web 3.0 the user owns the information. Decentralized Identity Documents (DID documents) allow users to create their own digital identity and decentralized cryptographic material resistant to quantum computing. A patient's DID document also contains a unique identifier for cross-border healthcare, endpoints for receiving DIDComm messages and for SOS services, and additional identifiers (passport, etc.). We propose a blockchain for cross-border healthcare to store the evidence of different electronic, physical identities, and identifiers, but also the rules approved by the patient or legal guardians to access patient data. The International Patient Summary (IPS) is the de facto standard for cross-border healthcare and includes an index of information classified into sections (HL7 FHIR Composition) that healthcare professionals and services can update and read on the patient's SOS service, then retrieving all the necessary patient information from the different FHIR API endpoints of different healthcare providers according to the approved rules.

Keywords. IPS, DID, PQC

1. Introduction

Using Web 3.0, health professionals are the generators and verifiers of health data, but the owners of these are the users, i.e., the patients and donors. At the same time, the information systems in the different organizations remain guarantors of the data and have custody of the information [1]. The International Patient Summary (IPS) [2][3] based on HL7 FHIR has been approved by G7 [4], E.U. and other countries as the standard for cross-border healthcare.

Both OpenID Connect (OIDC) [5], SMART-On-FHIR (SMART) [6] and Financial API Security Profile (FAPI) [7] are based on the JOSE standard. FHIR servers use OIDC for the authorization and identification of end-users (clinicians and patients) as specified in SMART. SMART defines asymmetric authentication ("private key JWT") to authenticate an end-user using a confidential app (client app) in a service provider (SP),

[1] Corresponding Author: Fernando Latorre Lopez, Conéctate Soluciones y Aplicaciones, S.L., Soria, CYL, Spain; Email: ferlatorre78@gmail.com.

using an asymmetric keypair. Furthermore, cryptographic material can be created using Post-Quantum Computing Cryptography (PQC) and the exchange of health data should be protocol agnostic, which must be done even if there is no TCP/IP connection, such as using Bluetooth or other methods (i.e. NFC or QR codes) [8].

2. Method

The data security is provided by the Post-Quantum Cryptography Standardization program and competition by NIST (National Institute of Standards and Technology in the USA), approved in 2022, which approves the first post-quantum computing resistant algorithms for data signing and encryption [9].

Decentralized Identity Documents (DID Documents) [10] enable different stakeholders to create their own cryptographic material, add different identifiers and generate a collision-free Universally Unique Identifier (UUID v4) for cross-border healthcare [11]. Evidence related with the identity of an entity or individual can be created, signed and stored in an immutable record by the issuer of the evidence.

The Hyperledger Fabric technology, which is a tool to create a private and permissioned blockchain network, can be used by different organizations for the auditable traceability of both identity data (electronic or physical documents and evidence) and cryptographic material related with every Universally Unique Identifier.

To standardize the way patients, legal guardians (e.g.: mother, father), health staff and other personnel can access data of a patient in the API service, Fhir API is introduced as FHIR documents that contain a FHIR Composition resource, which has an index of resources identified by both an UUID and the URL of the resource in a service provider (SP). FHIR API standardizes the way.

The JavaScript Object Signing and Encryption standards (JOSE) enable the definition of how the data exchanged can be signed (JWS) and then encrypted (JWE) [12] for authentication or data exchange. DID Communication (DIDComm) Messages extends JOSE specification for the traceability of the messages exchanged between a sender and a recipient, by adding “body”, “type”, “id” and other properties [13].

3. Discussion

Every client software application (personal or professional) can know both public asymmetric keys of an API service to send encrypted requests and to verify the response received by using the “*Well-known”* path of the API service, as defined in both OIDC, SMART and Well Known DID Configuration. This enables a client app to obtain the digital identity of the API service, the URLs of the endpoints and the features a server supports such as the FHIR capabilities defined in SMART.

The DID Documents of both entities and individuals can be stored in a blockchain network of federated organizations. In this way, every digital identity and access token issued in the federated network by some OpenID provider can be verified by any of the other parties in the network to allow access to a patient's health data. The event of this access can be stored in the blockchain network for auditing purposes.

The patient or legal guardians can define a SOS service in the patient's DID Document to allow healthcare providers to update the patient index each time a new record is created and to read the patient index in case of emergencies. The rules for

accessing the SOS index can be defined and signed by the patients themselves or by their legal guardians and stored in the blockchain through a FHIR Contract, so that the SOS service can verify if the applicant complies with the rules defined in the SOS Contract to disclose the entire index or specific information.

Although not defined in the current JOSE, OIDC, FAPI, FHIR, or DIDComm specifications, both DIDComm messages and post-quantum computing algorithms, (such as CRYSTALS-Dilithium and CRYSTALS-Kyber) can be used for signing and encryption, to extend current specifications as a secure envelope (see Figure 1) for information storage and exchange with resistance to quantum computers, regardless of the security of the transport protocol or storage provider. In this way, DIDComm messages can be used over both TCP/IP and Bluetooth connections and for confidential storage using Encrypted Data Vault (EDV), as illustrated in Figure 1 and Figure 2.

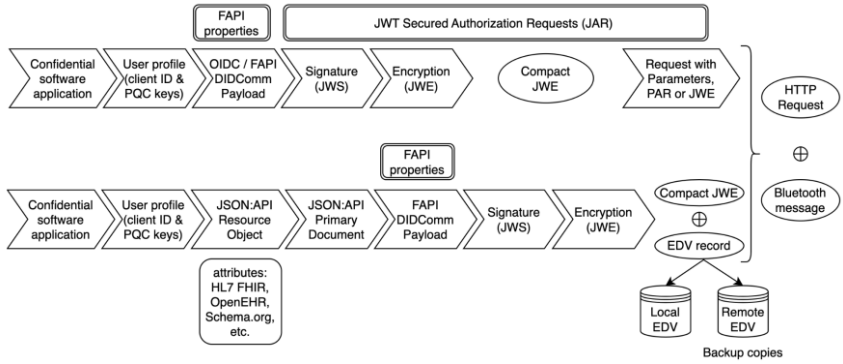

Figure 1. Secure data messaging using DIDComm for different data formats and protocols.

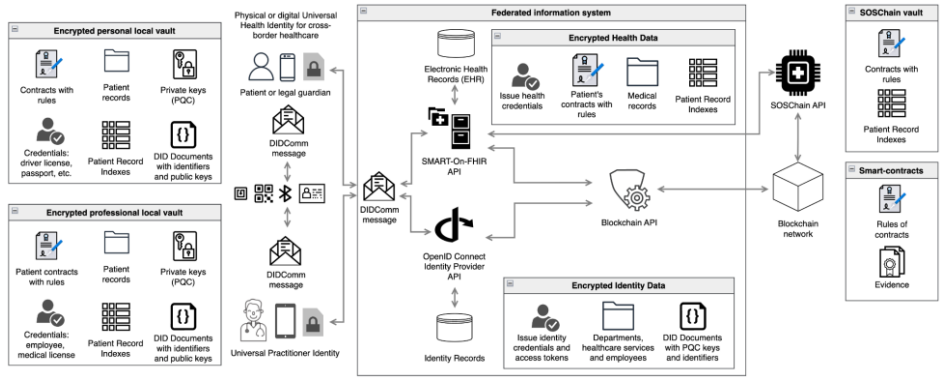

Figure 2. Cross-border healthcare using decentralized data, DIDComm messages and patient data index.

4. Conclusions

A patient or legal guardian (e.g., mother or father) as well as a professional working in a healthcare service of an organization (for example, a healthcare provider) can generate a decentralized identity with PQC algorithms in a confidential software application. The DID Document contains a unique identifier for cross-border healthcare and can include additional identifiers such as national identity document, passport, patient number,

insurance number, etc. Additionally, the patient or legal guardian(s) can define a SOS service in the patient's DID Document and a SOS Contract with the rules for accessing patient data in case of emergencies (FHIR Contract for SOS).

The audit record of decentralized identities, evidence, contracts and consents can be stored in the blockchain network through an OpenID Provider (OP) service available in the information systems of the federated organizations. The OP issues access tokens to healthcare personnel (employees) and to patients and legal guardians. A trained and authorized employee can verify the identity of both the patient and the legal guardian and register the evidence in both the OP and the blockchain network.

The SOS Contract with the rules for accessing patient data in emergencies is stored in the blockchain network by the patient or legal guardian through a federated information system. The practitioner can read the index of the patient's records in the SOS service if the rules allow it, retrieve them from different service providers, build a document with the medical records (IPS), generate new ones for the patient, update the patient's index with the new data generated, and send a notification to the patient or legal guardians, so they can retrieve the new records from the service provider in the updated patient's index.

References

[1] Latorre Lopez F, Sala Cano N, Fundación UNID et al., Universal Health Chain - v3. [Generated 2023 Feb 1]. Available from: https://github.com/Universal-Health-Chain/docs/tree/main/v3.

[2] CEN-CENELEC, New CEN standard TS 17288 'The International Patient Summary: Guideline for European Implementation', media release 2018, [posted 2018 Feb 16]. Available from: https://www.cencenelec.eu/news-and-events/news/2021/eninthespotlight/2021-02-16-ts-17288-the-international-patient-summary/.

[3] HL7 Foundation, Advancing the International Patient Summary, media release 2021, [posted 2021 Dec 1]. Available from: https://blog.hl7.org/advancing-the-international-patient-summary-ips.

[4] United Kingdom Department of Health and Social Care, G7 Research Group, G7 Health Track: Digital Health Final Reports, University of Toronto, 2021 [posted 2021 Dec 30]. Available from: http://www.g7.utoronto.ca/healthmins/2021-reports.html.

[5] Sakimura N et al., OpenID Connect Discovery 1.0 incorporating errata set 1, 2014 November 8. Available from: https://openid.net/specs/openid-connect-discovery-1_0.html.

[6] HL7 International, SMART App Launch 2.0.0, IG c2020, [generated 2023 Apr 18]. Available from: https://build.fhir.org/ig/HL7/smart-app-launch/app-launch.html.

[7] Consumer Data Standards, The Treasury, Government of Australia, Security Profile, [accessed 2023 March 19]. Available from: https://consumerdatastandardsaustralia.github.io/standards/#security-profile.

[8] Cano NS, Lopez FL, inventors; Conectate Soluciones y Aplicaciones, assignee. Procedure for the Global Unified Registration and Universal Identification of Donors, 2021 February 18, USPTO, US 17/178,966 2021/0174914, 2021 Jun 10.

[9] National Institute of Standards and Technology, U.S. Department of Commerce, NIST Announces First Four Quantum-Resistant Cryptographic Algorithms, media release, 2022 July 5. Available from: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

[10] Sporny M et al., Decentralized Identifiers (DIDs) v1.0, 2022 July 19, World Wide Web Consortium. Available from: https://www.w3.org/TR/did-core/.

[11] Latorre Lopez F, Sala Cano N, Conectate Soluciones y Aplicaciones SL,Unified Identification Protocol for Training and Health, Patent number US 11,636,776, 2023.

[12] Jones M et al., JSON Web Token (JWT), IETF RFC 7519, ISSN: 2070-1721.

[13] Curren S et al. DIDComm Messaging v2.x Editor's Draft, Decentralized Identity Foundation. Available from: https://identity.foundation/didcomm-messaging/spec/.