Interoperable Universal Resource Identifier for Selective Disclosure of Data

Fernando LATORREa,b,c,1, Claudia E HAWKSa, Bruno COLMENARESa, Deepika VERMAb, Marisa GILc, Nuria SALAb,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. All the information stored in the different information systems is issued in a format that allows the holder (the information owner) to disclose only certain information to a third party, which will act as a requester, receiver and verifier of the information disclosed by the holder. We define the Interoperable Universal Resource Identifier (iURI) as a harmonized method of representing a claim (minimum piece of verifiable information) using disparate encoding systems, agnostic to the original encoding system and data format. Encoding systems are represented in Reverse Domain Name Resolution (Reverse-DNS) format for HL7 FHIR, OpenEHR, and other data formats. The iURI can then be used in JSON Web Token for Selective Disclosure (SD-JWT) and Verifiable Credential (VC), among others. The method enables a person to demonstrate data that already exists in different information systems in disparate data formats, and even an information system, to verify certain claims, in a harmonized way.

Keywords. credentials, claims, disclosure

1. Introduction

Currently, neither the FHIR nor OpenEHR API services support selective disclosure of information or the ability of a patient or legal guardian to selectively add verifiable information, such as a passport or relationship to a minor (for example, mother or father).

As an example, a married woman giving birth to a child in a hospital is currently unable to obtain her information in a digital format that would allow her to later disclose only certain information to a third party for a specific purpose (information verifier). Some of the purposes may be: registration of the child in a civil registry or in an embassy, proof of being married to another person, proof of an identity document or passport of the mother and the newborn, the relationship of the parents with the child (i.e. birth parents, adoptive parents), etc.

Data minimization can be used in a similar way as defined in the SMART Health Cards (SHC) specification [1] to use only a limited set of claims, but can include claims not only from HL7 FHIR but also from other formats, for example, OpenEHR simSDT

1 Corresponding Author: Fernando Latorre Lopez; Email: ferlatorre78@gmail.com.
Applying some transformation rules to different data formats, specific pieces of information (claims) can be expressed as the pair “claim name” and “claim value”. Also, information can be shown as a Uniform Resource Identifier format for interoperability (iURI), which can also be used to set some specific verifiable information in an information system.

An individual (i.e., patient or donor, legal guardian, or an employee in a healthcare or other organization) using a software application can make a request to an Application Programming Interface service (API) to obtain specific information about an individual (i.e. patient). A Universal Resource Identifier (URI) can be used to represent minimal pieces of verifiable information (claims) in different data encoding systems, in an interoperable manner (i.e. by using reverse-DNS to represent the coding system). Next, a verifier can request specific claims to an API service, get approval from the data owner or legal guardian and get specific verified claims, in a harmonized way.

2. Method

Both OpenID Provider (OP) and FHIR API services are used to issue verifiable information of a patient, i.e., SMART Health Cards (SHC) [1]. SHC uses verifiable credential (VC) as tamper-evident electronic document with a cryptographically verifiable authorship that contains claims about the patient and JSON Web Signature (JWS) to secure the JSON-based claims expressed in a signed JSON Web Token (JWT) against modification.

Selective Disclosure for JSON Web Tokens (SD-JWT) [2] enables selective disclosure of claims in a signed JWT, enabling sharing only some specific claims (Disclosures) included in the original signedJWT instead of revealing all the information to every verifier. When issuing a SD-JWT to the holder, the issuer sends a JWT which contains the digests of the original data, but also the specific Disclosures of the data, which are concatenated to the JWT to conform the SD-JWT. It enables the holder to decide which claims will be disclosed to a verifier. The verifier has to verify that all disclosed claim names and claim values were part of the SD-JWT, using the Disclosures to extract the original JSON data and to check the digests over the source data in the JWT.

To enable patients (holders) or legal guardians to receive a SD-JWT from a FHIR endpoint, the requester shall notify the type of response expected by the client app to the endpoint, for example, by using the HTTP header “Accept sd-jwt”. In this way, the requester could be able to disclose only some elements of the FHIR resources.

The complex structure of the data returned by a FHIR search makes it difficult for holders to manage selective disclosure of information. An interoperable URI (iURI) is proposed as a harmonized method to get and verify electronic information, containing concrete claims encoded for specific coding systems through different data standards (HL7 FHIR, OpenEHR, and others).

An URI can be an URL (Uniform Resource Locator or web address, which specifies the location of a resource on a computer network), an URN (Uniform Resource Name, which is an Internet resource with a name that has persistent significance), or a DID (Decentralized Identifier).
3. Discussion and conclusion

The Method of a Universal Registration and Identification of Legal Procedures [4] proposes a harmonized way to represent data about a legal document in an URN. The URN proposed by this method can be extended and combined with both the “Consumer Data Standards” (CDS) [5] and the “did:web” [6] specifications for interoperability purposes. In this way, an interoperable URI (iURI) is defined as: uri-string = <kind-of-uri> “:” <uri-namespace> “:” <web-domain * (”.” path)> “:”<cds” (“.”<territory>) “:” <specification-version> “:” ( <sector> | <category> ) * (”.” <claim-reverse-DNS-name> “:” <claim-additional-type> “:” <claim-value> ).

The “uri-namespace” must be the same in different territories to be universal for cross-border healthcare. An universal health identifier of a person can be represented in a interoperable URI with the claim name “x-uhc-mid” as per the Unified Identification Protocol for Training and Health [7], where the uri-namespace can be set to “unid” (name of the foundation who manages the “x-uhc-mid” registration), the string “individual” is set in the issuer-web-urn part and the territory is removed from the cds part (it is global for cross-border healthcare): urn:unid:individual:cds:v1:identity:person:x-uhc-mid:uuid:<universal-health-identifier>

To resolve the DID Document of an entity (which contains the public cryptographic material), the interoperable URI can be converted to a DID simply by replacing the URI type from "urn" to "did".

Reverse-DNS format can be used to define both the claim name and the coding system used to represent the value of a claim. For example, a national identity document, passport, visitor permit, driver license, citizenship card, tax number, patient identifier, member number of an insurance policy, jurisdictional health number, medical doctor license, marriage certificate, birth certificate (among others) are defined in the HL7 table v2-0203 or “identifierType” [8] (NN, PPN, VP, DL, CZ, TAX, PI, MB, JHN, MD, MCT, BCT, respectively).


The conversion of a URN to another type of URI such as an URL can be done following the did:web method, where the maximum length for the URL is 2048 characters as per the HTTP specification. The URL shall be dynamically resolved by a service provider (SP) to process the claims included in the URL.

The interoperable claims defined in an interoperable URI can also be represented in a JSON object, where the claim-reverse-DNS-name is the name of the JSON property name and the value of the JSON property contains "<claim-additional-type>:<claim-value>". In this way, the interoperable claims can be used in both OpenID For Identity Assurance (OIDC4IDA), SD-JWT, Verifiable Claims, Verifiable Credentials (VC) and OpenID for Verifiable Credentials (OIDC4VC) specifications, among others.

Health claims in iURI format can be included in a VC as JSON data (FHIR, OpenEHR, etc). For example, the FHIR claims “Person.name.family”, “Person.name.given” [9] “Immunization.occurrenceDateTime”, “Immunization.status"
and “Immunization.vaccineCode” [10] can be contained in the “credentialSubject” element of a VC in order to generate an SD-JWT for these claims (adding the “_sd” element). For example, the unique universal identifier of the person (Japanese citizen) goes first (similar to a header of the data), then the “Person” claims (i.e. ICAO Doc9303 transliteration obtained the data of a passport), and finally, the clinical resource’s claims, both arranged alphabetically: { “x-uhc-mid”: “uuid:00000000-0000-4000-0000-000000000000”, “org.hl7.fhir.r4.Person.name.family”: “int.icao.doc9303.MRZ:KIMURA”, “org.hl7.fhir.r4.Person.name.given”: “int.icao.doc9303.MRZ:MICHIO”, “org.hl7.fhir.r4.Immunization.occurrenceDateTime”: “org.iso.8601:2023-01-30”, “org.hl7.fhir.r4.Immunization.status”: “org.hl7.fhir.valueset.immunization-status:completed”, “org.hl7.fhir.r4.Immunization.vaccineCode”: “no.whocc.atc:J07BX01” }.

SD-JWT is equivalent to an Issuer-signed W3C Verifiable Credential (W3C VC), where the Disclosures are sent alongside a VC. A Presentation of Disclosures with a Holder Binding JWT is equivalent to a Holder-signed W3C Verifiable Presentation (W3C VP). For example, a verifiable credential can be requested by a holder and created by the issuer containing in the “credentialSubject” element the interoperable claims for the subject (e.g.: person). Then the SD data (“_sd” element) can be added to the “credentialSubject” object and the algorithm used for SD to the properties of the JWT of the credential (“_sd_alg” property).

References

[1] SMART Health IT and Boston Children’s Hospital, SMART Health Cards, Available from: https://smarthealth.cards/