Exchange Purpose (XP) Implementation SOP: Individual Access Services (IAS): Demographic Matched

Version 2.0

DRAFT for Stakeholder Feedback

January 19, 2024

Applicability:
4.1, 4.2, and 4.3: IAS Providers Leveraging
Demographics-Based Patient Matching for Requests

4.4: QHINs, Participants, Subparticipants (for purposes of IAS Responses)

1 Common Agreement References

The requirements set forth in this Standard Operating Procedure (SOP) are required for implementation in addition to the terms and conditions found in the Common Agreement, applicable Framework Agreements, the Qualified Health Information Network™ (QHIN™) Technical Framework (QTF), and applicable SOPs, including the Exchange Purposes (XPs) SOP. The Trusted Exchange Framework and Common Agreement^{SM} (TEFCA^{SM}) Cross Reference Resource identifies which SOPs provide additional detail on specific references from the Common Agreement.

All documents cited in this SOP can be found on the Recognized Coordinating Entity® (RCE™) website.

2 SOP Definitions

Terms defined in this section are introduced herein and can be found in the TEFCA Glossary. Capitalized terms used in this SOP without definition shall have the respective meanings assigned to such term in the TEFCA Glossary.

This SOP includes no new definitions.

3 Purpose

This SOP identifies specific requirements that Individual Access Services (IAS) Providers are required to follow for Individual identity verification for IAS demographics-based matching. This SOP also identifies when a QHIN, Participant, or Subparticipant is required to Respond to an IAS Request made using demographics-based matching.[1] Requirements for IAS Requests made using Health Level 7® (HL7®) Fast Healthcare Interoperability Resources® (FHIR®) and OAuth with responder-issued credentials are out of scope for this SOP and are in the QTF. Privacy and security requirements for IAS Providers are also out of scope for this SOP and are in the IAS Provider Requirements SOP, along with the Common Agreement.

[1] Nothing in this SOP alters a Covered Entity's obligations under the HIPAA Rules.

4 Procedure

4.1 Credential Service Provider

IAS Providers MUST have an agreement with a credential service provider (CSP) who has been approved by an RCE-selected CSP approval organization.[2] The CSP approval organization must maintain a published list of CSPs who conduct identity proofing to at least Identity Assurance Level 2 (IAL2) as defined by the then latest version of the National Institute of Standards and Technology Special Publication 63A Digital Identity Guidelines (NIST SP800-63A). The CSP approval organization MUST require approved CSPs to be assessed for conformance to the minimum appropriate identity proofing and credential management standards, and to publish and maintain the standards to which the CSPs are assessed.

4.2 Authentication

IAS Providers MUST authenticate Individuals using processes set to at least Authenticator Assurance Level 2 (AAL2) as defined by the then latest version of the NIST SP800-63A requirements.

4.3 Identity Verification Requirement

IAS Providers MUST verify the identities of Individuals to at least IAL2 via a CSP prior to the Individual's first use of TEFCA Exchange, and then again after credentials expire.

a. Verification MUST include, at a minimum, the following demographics: First Name, Last Name, Date of Birth, Address, City, State, ZIP.

b. Verification SHOULD also include, but does not require, Sex, Middle Name, Middle Initial, Suffix, Email Address, Mobile Phone Number, Social Security Number (SSN), SSN last 4 digits, ZIP+4, and other verifiable identifiers (e.g., Medical Record Number, Passport Number, Driver's License, State ID).

c. IAS Providers MUST demonstrate that all Individuals that elect to use their IAS offering have proven their identities consistent with achieving IAL2. This evidence MUST be included within the Request as an IAL2 Claims Token using the OpenID Connect token format as further specified in Appendix A.

d. Requests initiated by an IAS Provider MUST include only the demographics as provided to the CSP and as part of the Individual's identity verified to IAL2.

[2] The RCE-selected CSP approval organizations will be published and maintained on the RCE website.

e. Historical name and/or address information MAY be included only if validated by the CSP for identity proofing for that Individual.

f. An IAS Provider MUST ensure that all updates to demographic information used for TEFCA Exchange for IAS have the demographics validated to IAL2 by the CSP prior to the Individual's first use.

4.4 Response Requirement

Any Responding Node that receives a Request from an IAS Provider that includes the appropriate IAL2 Claims Token, as specified in 4.3(c), and that achieves an acceptable demographics-based match based on responder policy is required to Respond with the Required Information per the Common Agreement, the QHIN Technical Framework, and the Exchange Purposes (XP) SOP.

Appendix A – Patient Request Identity Verification Policy

Overview

When processing Requests initiated by an Individual, it is imperative that the Individual's information is disclosed only to the Individual to whom that information pertains. This is typically accomplished by having the Individual authenticate directly with the Responding Node, but in cases where such an authentication workflow is either undesirable or infeasible, additional mechanisms are needed.

This Appendix details an exchange pattern within TEFCA in which an Initiating Node facilitating an IAS Request MUST partner with a credential service provider (CSP) to identity proof the Individual to at least IAL2 prior to sending Requests. The CSP MUST provide back to the IAS Provider a signed, technical token (IAL2 Claims Token) containing the Individual's demographics Node, as part of the IAL2 identity verification service. By policy, the IAS Provider's Initiating Node MUST provide this token within the Patient Discovery (XCPD) or FHIR transaction.

Trusted Credential Service Providers

IAS Providers that initiate IAS Requests MUST use one or more of an approved set of trusted CSPs that has been vetted and approved by a certifying body selected by the RCE, which will be authorized to perform IAL2 identity verification services. The RCE website will link to all approved certifying bodies. Each CSP will provide an endpoint to share a JSON Web Key Set (JWKS), which a Responding node MAY use to validate an identity token issued by that CSP. After verifying an Individual's identity on behalf of the IAS Provider, the CSP MUST make available to that IAS Provider a signed OpenID Connect token.

The Initiating Node MUST relay the CSP-provided OpenID Connect token within its Request using an additional SAML attribute statement ("id_token") containing the OpenID Connect token in a QHIN Query or as an additional element ("id_token") within the TEFCA_IAS extension in the FHIR Query.

OpenID Connect Token Construction (IAL2 Claims Token)

OpenID Connect is an authentication protocol that specifies how to exchange a user's identity. OpenID Connect closely integrates with the OAuth 2.0 authorization method. By specifying its use in TEFCA Exchange, we anticipate and align the exchange of Individual identity with future exchange methods. In healthcare, OpenID Connect is built into the HL7 SMART on FHIR specification and is also the *de facto* standard for FHIR exchange internationally.

The OpenID Connect Core specification describes many optional capabilities. This specification makes use of OpenID Connect's ID Token. The following requirements apply:

- Public Keys Published as Bare JWK Keys: The CSP MUST publish public keys as bare JWK keys (which MAY also be accompanied by X.509 representations of those keys).

- Signed ID Token: The CSP MUST support Signing ID Tokens with RSA SHA-256.

- Claims: The CSP MUST include the below claims.

Table 1: OpenID Connect (OIDC) JWT headers

OIDC JWT Header	
alg	Hardcoded to “RS256”.
kid	Identifies which key to use from the JWKS.
typ	Hardcoded to “JWT”.

OIDC JWT Body	**Description**
aud	HCID of the IAS Provider as a URI. For example urn:oid:<oid> (per RFC 3001).
iat	When the CSP issued the token.
iss	The base URL of the CSP at which the JWKS is accessible.
jti	Unique identifier for the JWT.
Demographics that MUST be included or use “Unknown” in your Request	
given_name	
family_name	
date of birth	
address	See list and definition of address elements, below. Allow multiple addresses (array) if supported by the CSP.
Demographics that MUST be included if known	
historical_address	See list and definition of address elements, below. Allow multiple addresses (array) if supported by the CSP.
middle_name	
middle initial	
suffix	
email	
phone_number	
SSN	
SSN Last four digits	
ZIP+4	
Sex	

OIDC JWT Body Address Object	Optionality
formatted	OPTIONAL
street_address	REQUIRED, IF KNOWN
city	REQUIRED, IF KNOWN
state	REQUIRED, IF KNOWN
zip_code	REQUIRED, IF KNOWN
country	REQUIRED, IF KNOWN

Example OIDC JWT

```
{
"alg":"RS256",
"kid":"toW9jMUSN/5/L3iwaQGdTmNDuhvp/JcAZVH/RGF2aWQgUHlrZQ==",
"typ":"JWT"
} {
"aud":"hci1",
"iat":1666280632,
"iss":”https://csp.example.com”,
“sub”:” f7bdf590-2fc4-4718-8f33-043c8f96b66d”,
“jti”:”bcb9533e-1cc1-48bd-848b-b4200ea504b9”,
“given_name”:”John”,
“family_name”:”Schmidt”,
“middle_name”:”Jacob Jingleheimer”,
“nickname”:”Ed”,
“email”:”jjjs@example.com”,
“email_verified”:true,
“phone”:”555-555-5555”,
“gender”:”M”,
“birthdate”:”Unknown”,
“address”:{
      “formatted”:”1060 West Addison Street, Chicago, IL 60613 USA”,
      “street_address”:” 1060 West Addison Street”,
      “locality”:”Chicago”,
      “region”:”Illinois”,
      “postal_code”:”60613”,
      “country”:”USA”
      },
“http://rce.sequoiaproject.org/OIDC/claim/mothers_maiden_name”:”Vetter”,
“http://
rce.sequoiaproject.org/OIDC/claim/principle_care_provider_id”:”29384572342”,
“http:// rce.sequoiaproject.org/OIDC/claim/birth_place_address”: {
      “formatted”:”1060 West Addison Street, Chicago, Illinois 60613 USA”,
      “street_address”:”1060 west Addison Street”,
      “locality”:”Chicago”,
      “region”:”Illinois”,
      “postal_code”:”60613”,
      “country”:”USA”
      },
“http:// rce.sequoiaproject.org/OIDC/claim/birth_place_name”:”Peaceful Valley
Hospital”
}
```

JSON Web Key Set URL

The CSP signs with a private key and publishes the corresponding public key at <iss>/.well-known/openid-configuration per OpenID Connect Discovery. For example, if the ID token's iss element is https://csp.example.com, the CSP's JSON Web Key Set (JWKS) document would be available at: https://csp.example.com/.well-known/openid-configuration.

Initiating Nodes and Responding nodes MAY use the public key to verify the CSP's signature on demographics included in the JWT. Therefore, the CSP MUST provide the JWKS publicly without requiring authentication.

CSP are encouraged to rotate encryption keys as described in OpenID Connect Core.

VERSION HISTORY

Version	Revision Date	Section #(s) of Update
Version 1.0	Released September 2022	N/A
draft Version 2.0	Released 1/19/24	All sections