

TOP-KT-016 - SMART on FHIR Conformiteit

✓ Versiegeschiedenis...

Versie	Datum	Status	Wijzigingen
1.0.0	27 Feb 2023	definitief	

Beschrijving

Binnen Koppeltaal is het van belang dat een 'SMART on FHIR' server implementatie precies aangeeft wat het kan (Capability). Clients kunnen vervolgens bij de server diens capabilities opvragen.

Overwegingen

Well-known URLs

In eerdere versies van SMART werden sommige van deze details ook overgebracht via de **CapabilityStatement** van een FHIR server. Hoewel de **CapabilityStatement** van toepassing is voor het uitwisselen van de capaciteiten rond de FHIR resources, is **dit mechanisme is volgens SMART on FHIR nu verouderd en dient daarom niet meer gebruikt te worden**. In Koppeltaal kiezen we voor de Well-Known Uniform Resource Identifiers (URI's) aanpak. De server MOET de FHIR OAuth-autorisatie endpoints en eventuele optionele SMART-mogelijkheden die hij ondersteunt overbrengen met behulp van een **Well-Known Uniform Resource Identifiers** (URI's) JSON-bestand.

Capability Set

In de [SMART on FHIR OAuth authorization Endpoints and Capabilities](#) worden Capability Sets besproken. Koppeltaal maakt gebruik van de Capability Sets, waarmee aangeven wordt wat de FHIR resource service en autorisatie service ondersteund. Koppeltaal maakt gebruik van de standaard waarden, m.u.v. de launch context; deze is in Koppeltaal gebaseerd op HTI.

Launch context

Koppeltaal maakt gebruik van HTI om de context van de launch vast te stellen, deze wordt aangeduid met de capability `context-ehr-hti`, deze is specifiek voor Koppeltaal.

Toepassing en restricties

Het opvragen van de conformiteit kan uitgevoerd worden zonder access token

Well-known URLs

De autorisatie endpoints die door een FHIR-bronserver worden geaccepteerd, worden weergegeven als een Well-Known Uniform Resource Identifiers (URI's) ([RFC5785](#)) JSON-document.

FHIR-endpoints die **autorisatie vereisen**, MOETEN een JSON-document weergeven op de locatie die wordt gevormd door /.well-known/smart-configuration toe te voegen aan hun basis-URL. In tegenstelling tot bijlage B.4 van RFC5785 kan de .well-known path-component worden toegevoegd, zelfs als het FHIR-endpoint al een path-component bevat.

Antwoorden voor /.well-known/smart-configuration-verzoeken ZULLEN JSON zijn, ongeacht de Accept-headers die in het verzoek zijn opgegeven.

De **Accept** header mag worden weggelaten, omdat de waarde altijd application/json zal zijn.

Multi-tenancy

Opvragen van SMART major versie 2 configuratie per domein (zorgafnemer). Basis URL

```
http://fhir.koppeltaal.nl/domeinzorgafnemer/v2
```

```
GET domeinzorgafnemer/v2/.well-known/smart-configuration HTTP/1.1
```

```
Host: fhir.koppeltaal.nl
```

Response op configuratie aanvraag.

Een JSON-document moet worden geretourneerd met het type application/json mime.

meta element	verplicht	Beschrijving
issuer	Ja	De Base URL van de autorisatie service.
jwtks_uri	Ja	De URL van de JSON Web Key Store (JWKS) van de autorisatie service.
authorization_endpoint	Ja	URL naar het OAuth2-autorisatie-endpoint.
grant_types_supported	Ja	matrix van ondersteunde typen toekenning op het token-endpoint. De opties zijn: <ul style="list-style-type: none">• "authorization_code" (wanneer SMART App Launch wordt ondersteund) en• "client_credentials" (wanneer SMART Backend Services wordt ondersteund).
token_endpoint	Ja	URL naar het OAuth2-tokenendpoint.

token_endpoint_auth_methods_supported	ja	Vaste waarde: <code>private_key_jwt</code>
registration_endpoint	niet gebruiken	
scopes_supported	Ja	Let op: de <code>system/*.cruds</code> scope wordt gezet door de auth server, en niet door de client zelf gezet. De SMART on FHIR backend service bepaalt de scope op basis van de applicatie-instantie rol. "openid", "launch", "fhirUser", "system/*.cruds", "system/*.cruds?resource-origin="
response_types_supported	Ja	<code>[code]</code>
management_endpoint	Ja	URL naar domeinbeheer
introspection_endpoint	Ja	URL naar het introspectie-endpoint van een server dat kan worden gebruikt om een token te valideren.
revocation_endpoint	niet gebruiken	
capabilities	Ja	Zie onderdeel capabilities sets . <ul style="list-style-type: none"> • launch-ehr • authorize-post • client-confidential-asymmetric • sso-openid-connect • context-ehr-hti • permission-v2
code_challenge_methods_supported	Ja	<code>["S256"]</code>

LET OP: Elk domein krijgt zijn eigen endpoints.

Eisen

[CNF - Eisen \(en aanbevelingen\) voor de conformiteit](#)

Voorbeelden

Response SMART Config

```

1 HTTP/1.1 200 OK
2 Content-Type: application/json
3
4 {
5   "issuer": "https://fhir.koppeltaal.nl/domeinzorgafnemer/v2",
6   "jwks_uri": "https://fhir.koppeltaal.nl/domeinzorgafnemer/v2/.well-known/jwks.json",
7   "authorization_endpoint": "https://fhir.koppeltaal.nl/domeinzorgafnemer/v2/auth/authorize",

```

```

8  "management_endpoint" : "https://domain-admin.koppeltaal.headease.nl",
9  "grant_types_supported": [
10     "authorization_code",
11     "client_credentials"
12 ],
13 "token_endpoint": "https://fhir.koppeltaal.nl/domeinzorgafnemer/v2/auth/token",
14 "token_endpoint_auth_methods_supported": ["private_key_jwt"],
15 "scopes_supported": ["openid", "launch", "fhirUser", "system/*.cruds", "system/*.cruds?resource-
origin="],
16 "response_types_supported": ["code"],
17 "introspection_endpoint": "https://fhir.koppeltaal.nl/domeinzorgafnemer/v2/auth/introspect",
18 "capabilities": [
19     "launch-ehr",
20     "authorize-post",
21     "client-confidential-asymmetric",
22     "sso-openid-connect",
23     "context-ehr-hti",
24     "permission-v2"
25 ],
26 "code_challenge_methods_supported": ["S256"]
27 }

```

Links naar gerelateerde onderwerpen

OpenID configuratie: [Ldapwiki: Openid-configuration](#)

{}