PCM
Patient Consent Manager

DR MVP1

15.1.26

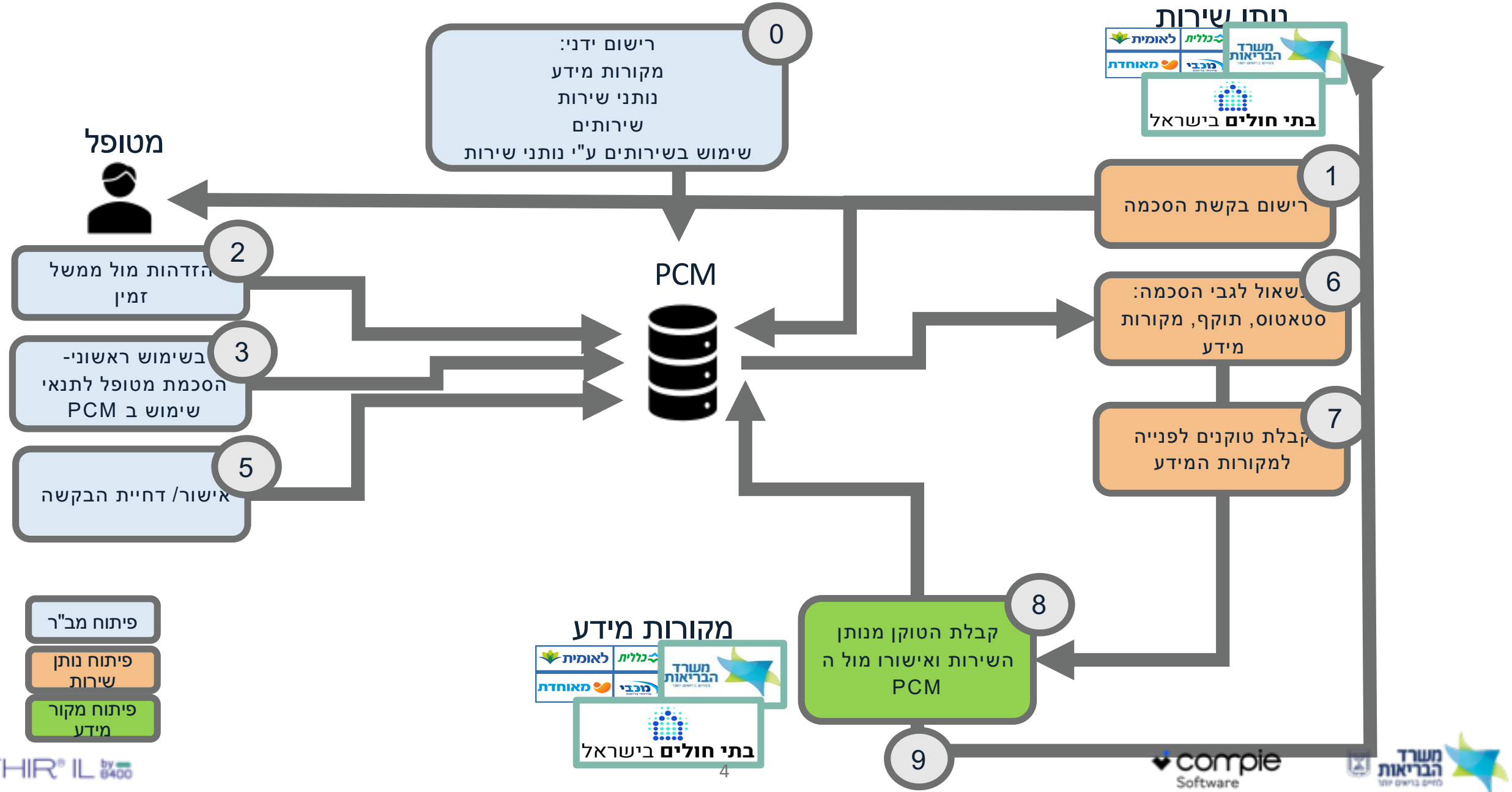
אג'נדה

- MVP1- לו"ז ותכולות
- תזכורת: תהליך הזדהות מול PCM
- הרשאה ואכיפת הסכמה במערכת PCM
- שאלות

תוכנית עבודה ארגונים PCM

	משימה	Oct 25	Nov 25	Dec 25	Jan 26	Feb 26	Mar 26	26 Q2	26 Q3	26 Q4	27 Q1	27 Q2	Jul 27
MVP1													
	DR- מקור מידע												
	פיתוח ממשק- מקור מידע												
	DR- נותן שירות												
	פיתוח ממשק- נותן שירות												
	בדיקות												
	מוכנות לאינטגרציה מול מב"ר												
	אינטגרציה מול מב"ר								אפריל- יולי				
שלב 2													
	DR												
	פיתוח- מקור מידע												
	פיתוח- נותן שירות												
	בדיקות												
	אינטגרציה מול מב"ר										נובמבר-מרץ		
עלייה לייצור	עלייה לייצור												

תבולות MVP1


0
רישום ידני:
מקורות מידע
נותני שירות
שירותים
שימוש בשירותים ע"י נותני שירות
נותני שירות
בתי חולים בישראל
מטופל
1
רישום בקשת הסכמה
2
הזדהות מול ממשל זמין
PCM
3
בשימוש ראשוני- הסכמת מטופל לתנאי שימוש ב PCM
5
אישור/ דחיית הבקשה
6
שאול לגבי הסכמה:
סטאטוס, תוקף, מקורות מידע
7
קבלת טוקנים לפנייה למקורות המידע
8
קבלת הטוקן מנותן השירות ואישורו מול ה PCM
9
מקורות מידע
בתי חולים בישראל
פיתוח מב"ר
פיתוח נותן שירות
פיתוח מקור מידע

תכולות MVP1

מוכנות לאינטגרציה : אפריל 26

מקור מידע

- הכנת תשתית MTLS
- הנפקת תעודה זמנית PEM לסביבת טסט (ללא private key) ושליחת התעודה למב"ר במייל
- הטמעת 2 תעודות ממב"ר בתשתית mtls: PCM, MOH
- קבלת הטוקן מנותן השירות ואישורו מול ה PCM (8)
- שליחת המידע לנותן השירות (9)

נותן שירות

- **רישום בקשת הסכמה (1)**
- **תשאול לגבי הסכמה: סטאטוס, תוקף, מקורות מידע (6)**
- **קבלת טוקנים מה PCM לפנייה למקורות המידע (7)**

רישום בקשת הסכמה

לינק לסוואגר

לינק לסימפליפייר (מראה פרופילים)

תשאול לגבי הסכמה

לינק לסוואגר

לינק לסימפליפייר (מראה פרופילים)

תהליך הזדהות מול PCM

- הארגון מחזיק תעודה דיגיטלית (Certificate) שנרשמה במאגר האמון הלאומי (NTN) התעודה כוללת מפתח ציבורי, והארגון שומר אצלו את המפתח הפרטי התואם.
- יצירת JWT Assertion – הארגון יוצר מסמך חתום דיגיטלית (JWT) המהווה הוכחת זהות. החתימה נעשית באמצעות המפתח הפרטי של הארגון.
- פתיחת חיבור מאובטח (mTLS) – הארגון ומערכת PCM מקיימים תקשורת הדדית מוצפנת, שבה כל צד מאמת את זהותו באמצעות התעודה הדיגיטלית שלו. ה־JWT נשלח בערוץ ה־mTLS למערכת PCM.
- אימות במערכת PCM – המערכת שולפת מה־NTN את המידע הציבורי על הארגון (תעודה / מפתח ציבורי), מאמתת את חתימת ה־JWT ומוודאת שהתעודה תקפה ולא בוטלה – מול ה NTN.
- הנפקת Access Token זמני – לאחר אימות מוצלח, המערכת מנפיקה לארגון אסימון גישה קצר טווח, המשמש אותו לקריאות עתידיות לממשקי ה־API של PCM (למשל FHIR). תוקף הטוקן 30 שניות

תהליך הזדהות מול PCM

דוג' לקריאה למערכת באמצעות ה JWT:

HTTP GET `[PCM FHIR BASE]/.well-known/smart-configuration`

Response:

```
}
"  authorization_endpoint" :"[PCM AUTHORIZATION BASE]/authorize,"
"  token_endpoint" :"[PCM AUTHORIZATION BASE]/token,"
```

POST`" authorization_endpoint"`
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&
client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer&
client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9&....
scope=consent.read consent.write fhir.read

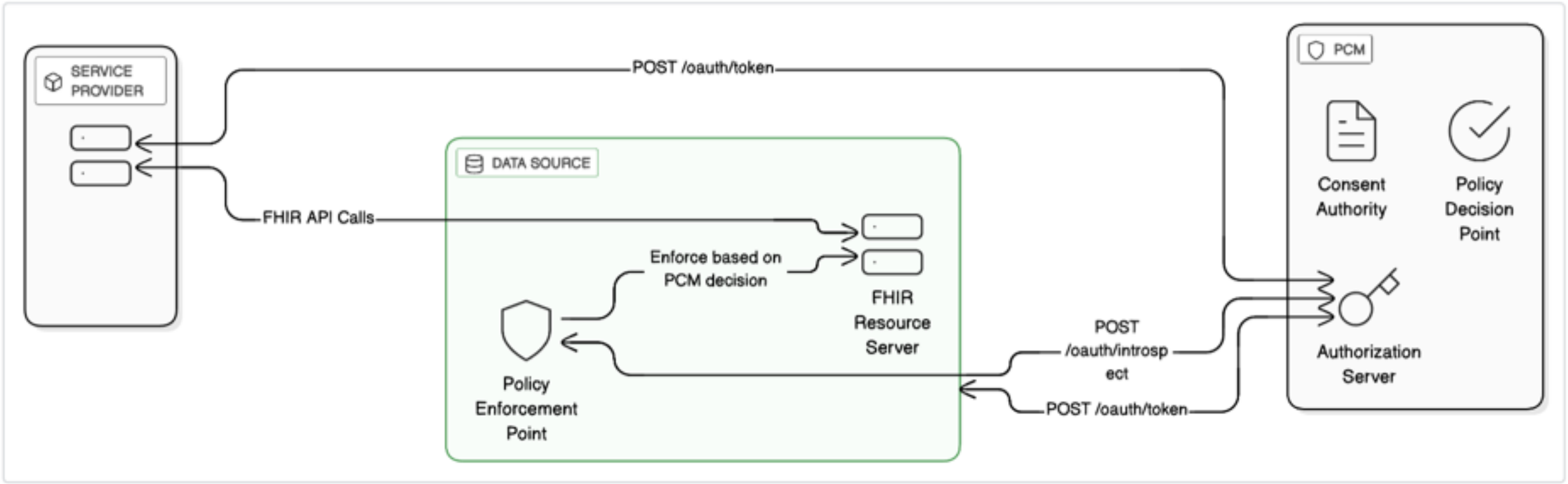
Authentication JWT Claims		
iss	required	Issuer of the JWT -- the client's client_id, as determined during registration (note that this is the same as the value for the sub claim)
sub	required	The client's client_id, as determined during registration with the FHIR authorization server (note that this is the same as the value for the iss claim)
aud	required	PCM authorization server's "token URL" (i.e. - `[PCM AUTHORIZATION BASE]/token`)
exp	required	Expiration time integer for this authentication JWT, expressed in seconds since the "Epoch" (1970-01-01T00:00:00Z UTC). This time SHALL be no more than five minutes in the future.
jti	required	A nonce string value that uniquely identifies this authentication JWT.

תהליך הזדהות מול PCM

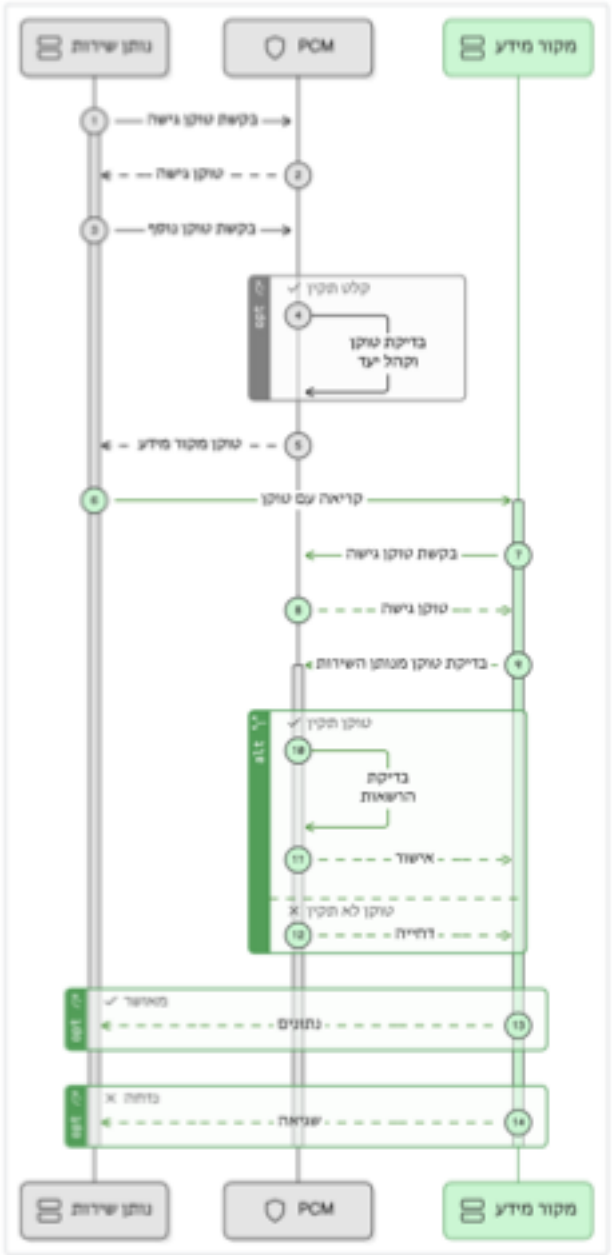
דוג' לתגובה של ה PCM עם Bearer token


```
}
"  access_token": "eyJraWQiOiIxMjM0NTYiLCJhbGciOiJSUzI1NiJ9,"...
"  token_type": "Bearer,"
"  expires_in": 30,
"  scope": "consent.read consent.write fhir.read"
{
```

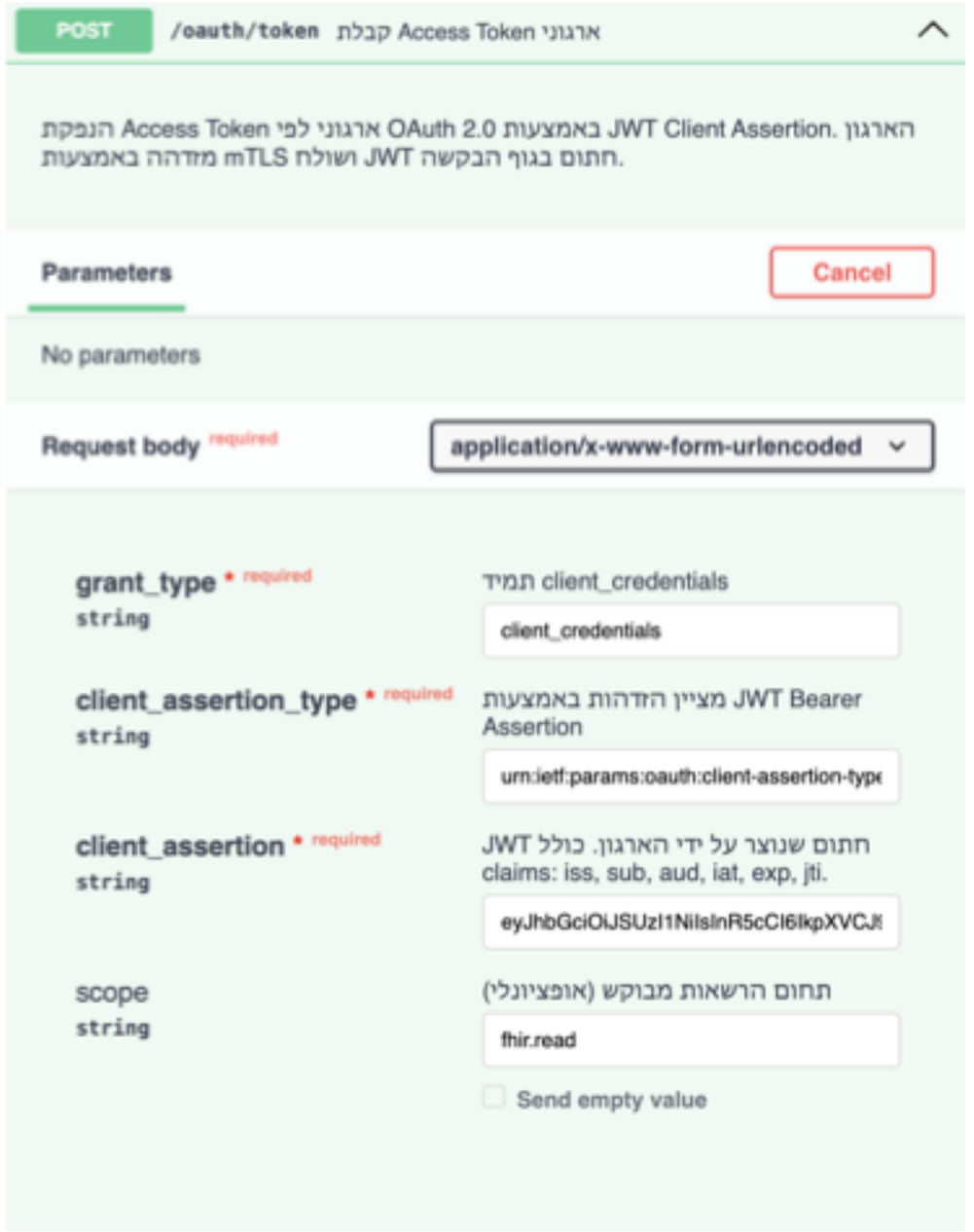
הרשאה ואכיפת הסכמה במערכת PCM



הרשאה ואכיפת הסכמה במערכת PCM



הזדהות מול PCM



הזדהות מול PCM

Responses

Code	Description	Links
200	טוקן הונפק בהצלחה	*No links*

Media type

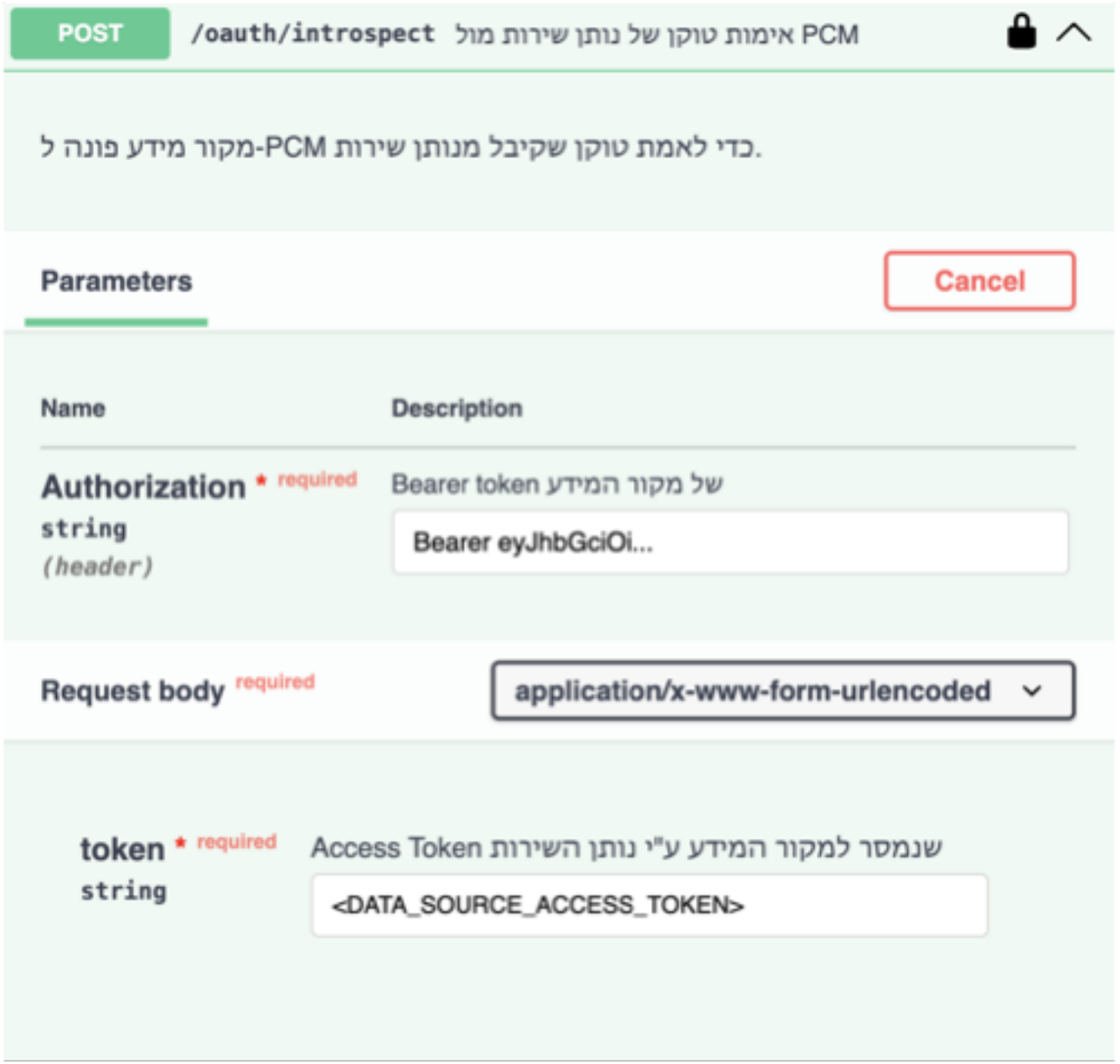
application/json

Controls `Accept` header.

Example Value | Schema


```
{
  "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6
IkpXVCJ9...",
  "token_type": "Bearer",
  "expires_in": 30,
  "scope": "fhir.read"
}
```

ולידציה של טוקן שהתקבל אצל מקור המידע



ולידציה של טוקן שהתקבל אצל מקור המידע

Responses

Code	Description	Links
200	תוצאת אימות הטוקן וההרשאה Media type application/json Controls Accept header. **Example Value** | Schema	*No links*


```
{
  "active": true,
  "patient": "http://fhir.health.gov.il/identifier/il-national-id|000000018",
  "aud": "https://fhir.maccabi4u.co.il/R4",
  "iss": "https://pcm.fhir.health.gov.il/",
  "token_type": "bearer",
  "scope": "patient/Encounter.rs?_security=http://fhir.health.gov.il/cs/hdp-information-buckets|EncounterInformation&date=ge2024-01-01",
  "client_id": "http://pcm.fhir.health.gov.il/organization/633",
  "expires_in": 3600,
  "iat": 1633532014,
  "exp": 1633535614,
  "jti": "550e8400-e29b-41d4-a716-446655440000",
  "intent": "http://pcm.fhir.health.gov.il/healthcareservice/269321"
}
```

הפגישות הבאות

- התנעת אינטגרציה לתכולות MVP1 – 24.3.26

FHIR® IL by 8400

משרד הבריאות
לחיים בריאים יותר

תודה רבה!