PCM
Patient Consent Manager

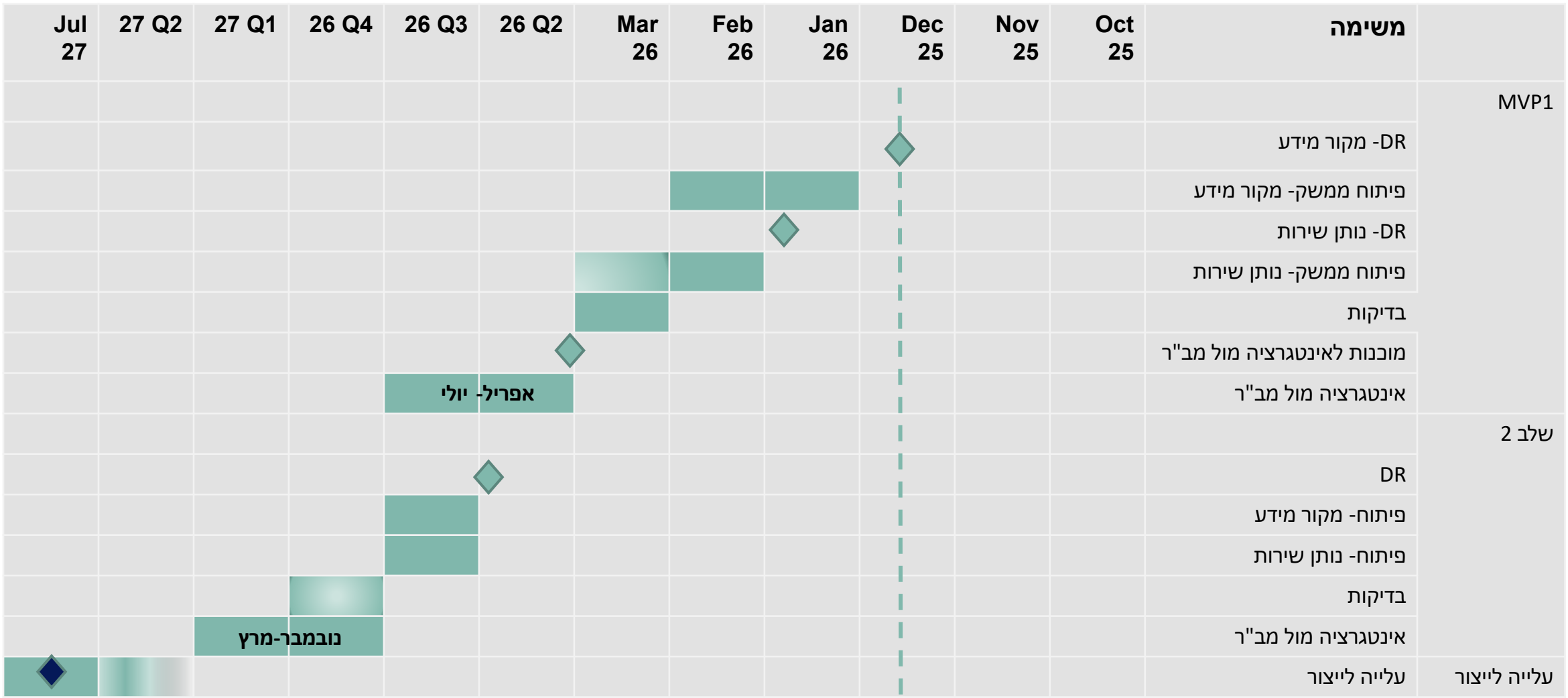
DR MVP1

18.12.25

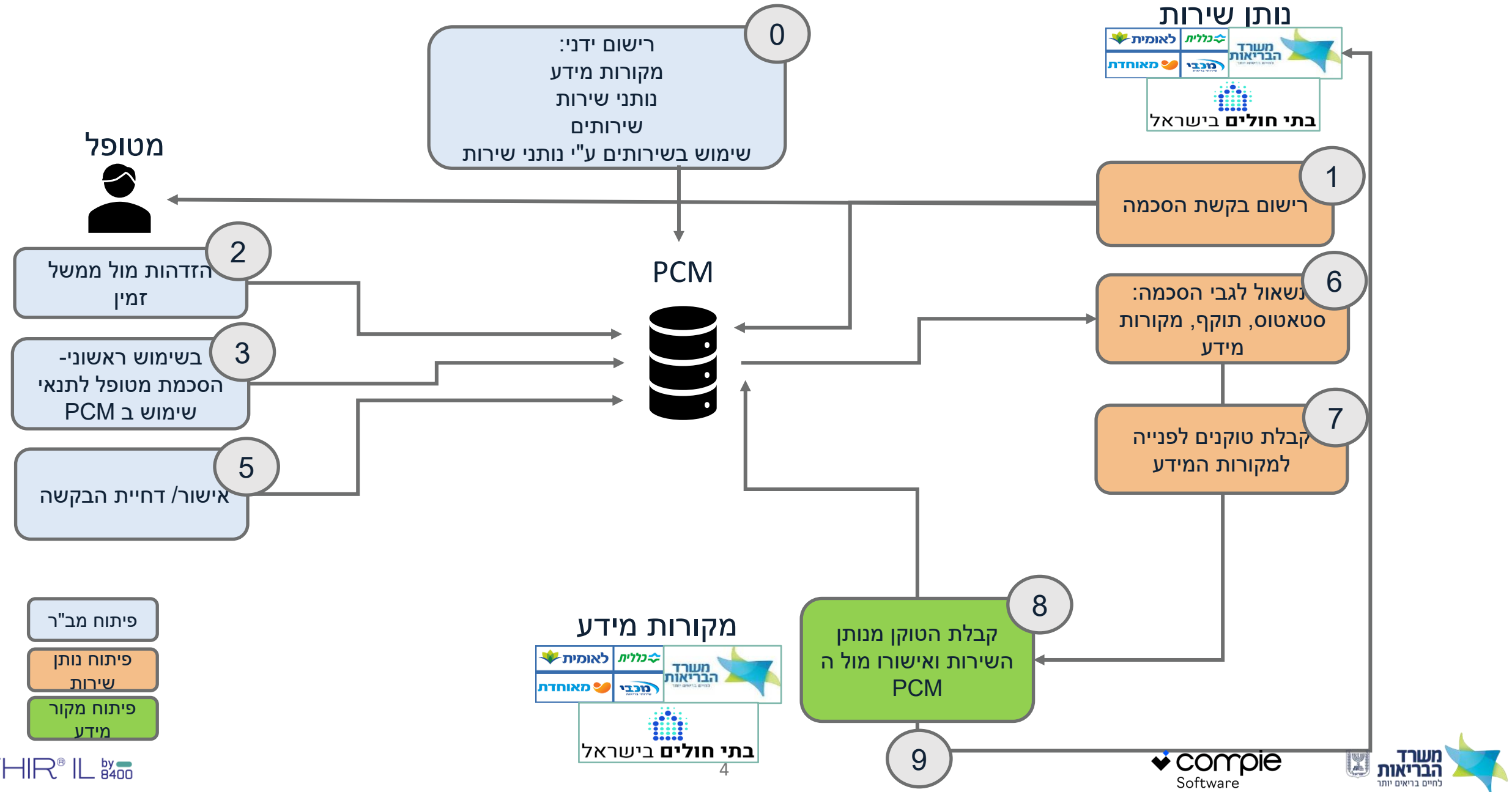
אג'נדה

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

תוכנית עבודה ארגונים PCM



תכולות MVP1


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

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

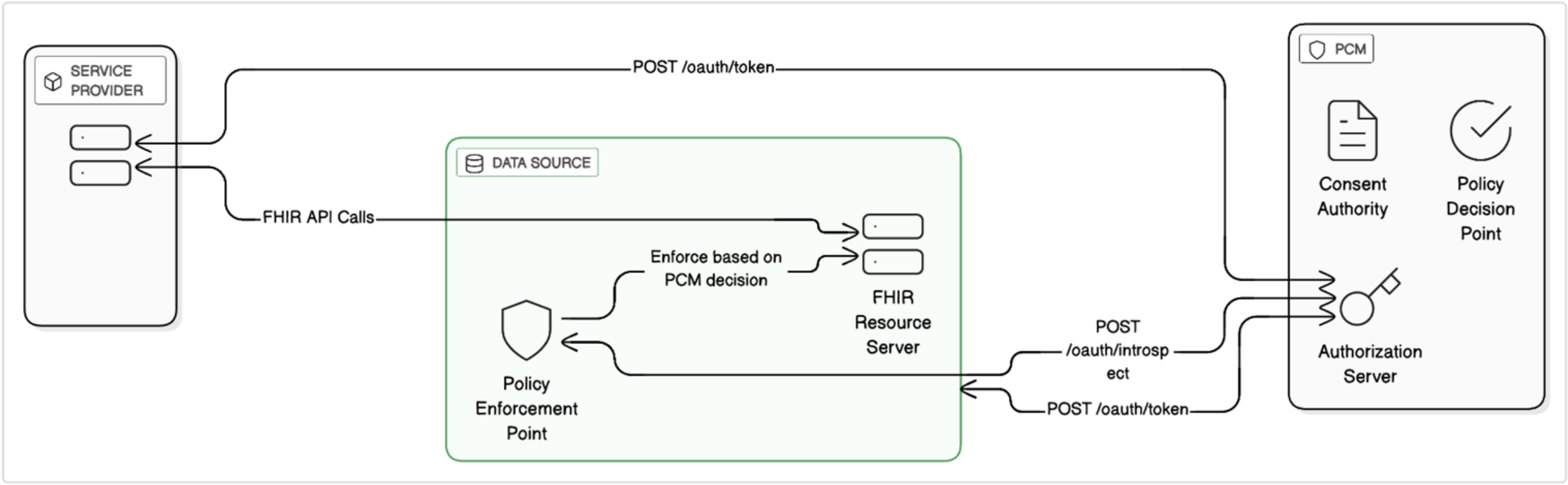
Authentication JWT Claims		
iss	required	Issuer of the JWT -- the client's client_id, as determined during registration (note that this is the same as the value for the sub claim)
sub	required	The client's client_id, as determined during registration with the FHIR authorization server (note that this 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

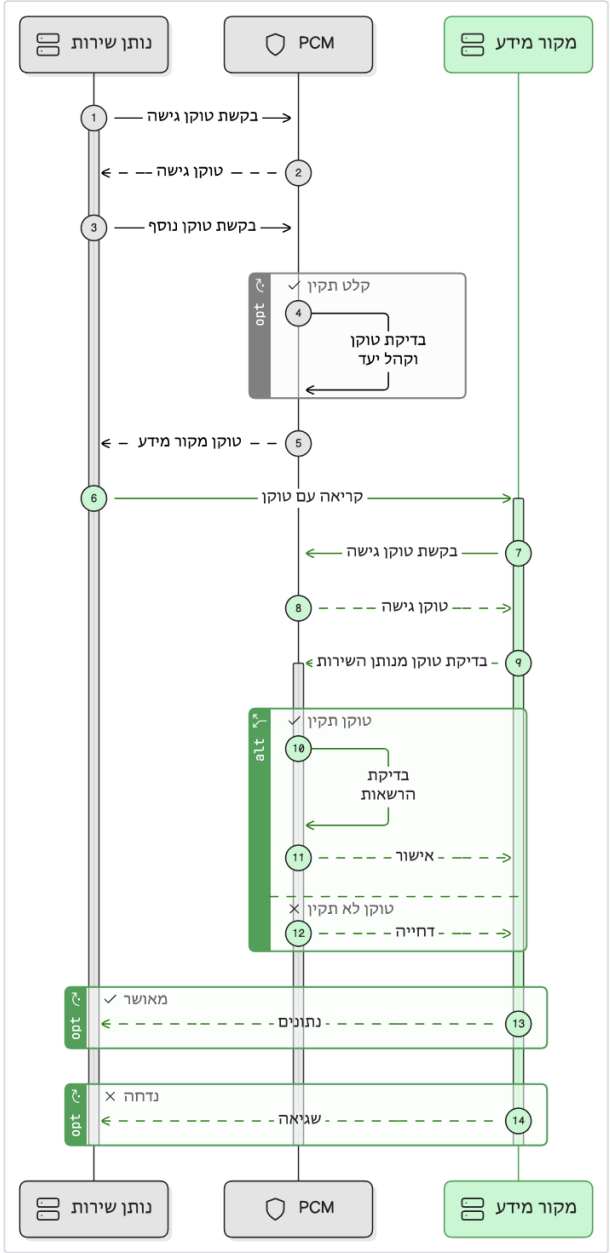
דוג' לתגובה של ה PCM עם Bearer token


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

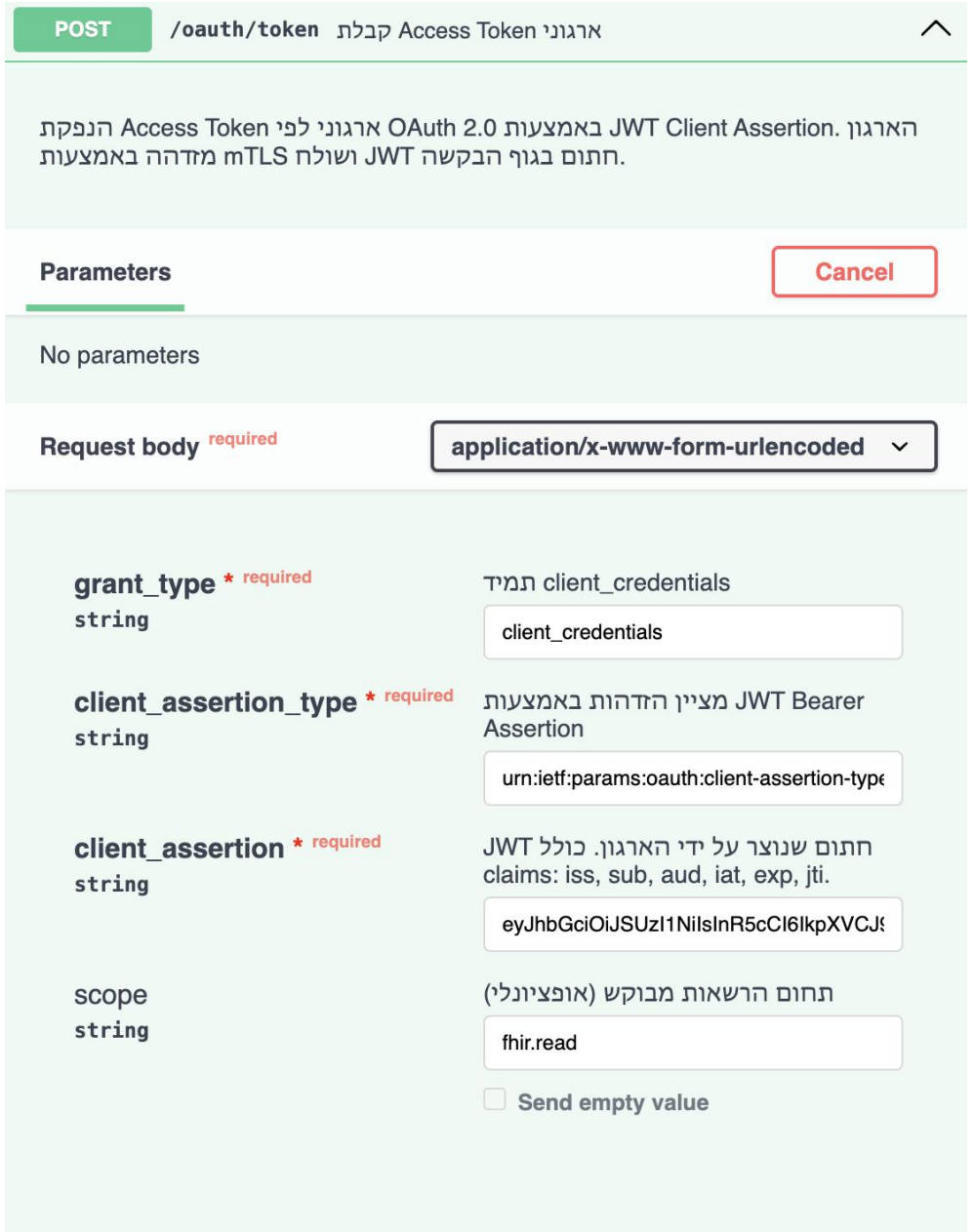
הרשאה ואכיפת הסכמה במערכת PCM



הרשאה ואכיפת הסכמה במערכת PCM



הזדהות מול PCM



FHIR® IL by 8400

compie Software

משרד הבריאות לחיים בריאים יותר

הזדהות מול PCM

Responses

Code	Description	Links
200	טוקן הונפק בהצלחה	*No links*

Media type

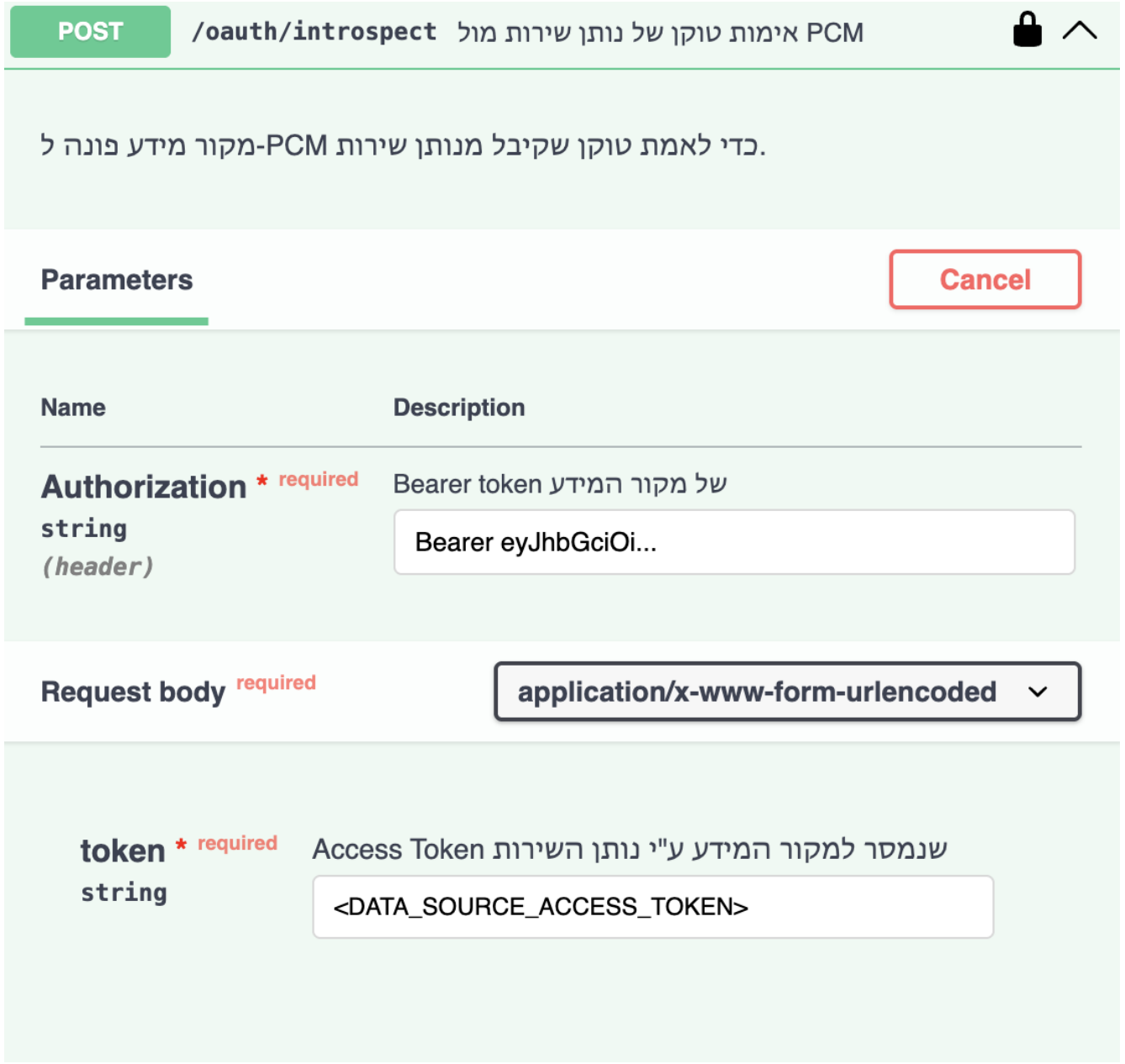
application/json

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"
}
```

MoH test service provider will send the following **Request**:

- **HTTP GET** `[Data Source FHIR BASE]/Patient?identifier=http://fhir.health.gov.il/identifier/il-hdp-test-id|1`
- The request will also include bearer token from PCM

Data source flow:

1. Receive **HTTP GET** request with bearer token from MoH test service provider
2. Authenticate to PCM using its own certificate and get **PCM access token**
3. With PCM access token as **bearer** do **HTTP POST** `[PCM AUTHORIZATION BASE]/introspect` sending access token from service provider

POST /introspect HTTP/1.1

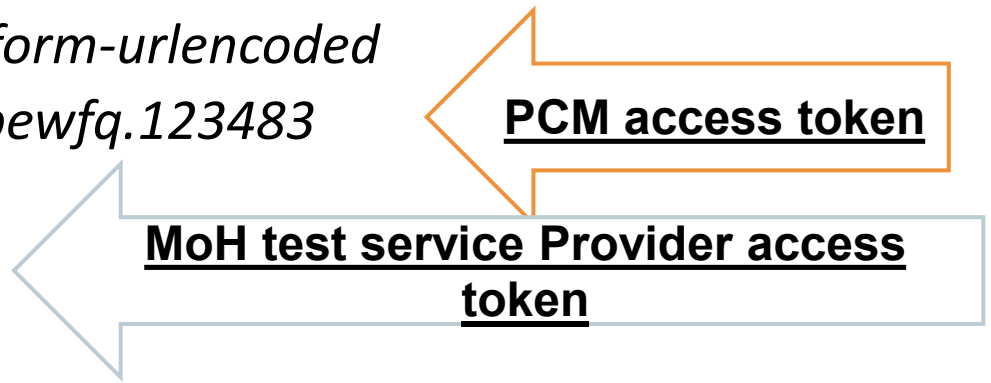
Host: pcm-example.fhir.health.gov.il

Accept: application/json

Content-Type: application/x-www-form-urlencoded

Authorization: Bearer 23410913-abewfq.123483

token=2YotnFZFEjr1zCsicMWpAA



Response from PCM (introspection)


```
{
  "active": true,
  "patient": "http://fhir.health.gov.il/identifier/il-hdp-test-id|1",
  "aud": "https://fhir.health-org-fhir-server.co.il/R4",
  "iss": "https://pcm.fhir.health.gov.il/",
  "token_type": "bearer",
  "scope": "patient/Patient.rs?_security=http://fhir.health.gov.il/cs/hdp-
information-buckets|patientDemographics",
  "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"
}
```


Replace with internal logical id

Server enforces scopes

Data source Response

- Data source should send back the synthetic test Patient resource with identifier “1” (as defined in technical requirements document in paragraph 3.10.1)
- The actual contents of the Patient resource does not matter for the integration test and can be anything – as long as it is a valid FHIR Patient resource and it has identifier *http://fhir.health.gov.il/identifier/il-hdp-test-id|1*

1. Subject Information (Distinguished Name — DN)

Field	Required?	Example	Notes
CN – Common Name	Yes	https://TestOrgPCM.TLS.gov.il	For TLS server: hostname / FQDN.
O – Organization	Yes	Test Org	Legal organization name.
OU – Organizational Unit	Yes	Test Org ICT	Internal grouping.
C – Country	Yes	IL	ISO-3166 2-letter code.
L – Locality/City	Yes	Tel Aviv	

2. Subject Alternative Names (SAN)

Required types:

- **DNS Names**:
  - https://TestOrgPCM.TLS.gov.il.gov.il
  - https://api.TestOrgPCM.TLS.gov.il.gov.il

Note: CN is obsolete for hostname validation; SAN is authoritative.

3. Key Parameters

Parameter	Example	Notes
Key Algorithm	ECDSA P-256	Most common: RSA 2048/3072; ECDSA P-256/P-384.
Key Size / Curve	ECDSA SECP-256	Must match policy.
Key Usage (KU)	digitalSignature	Restricts operations allowed.
Extended Key Usage (EKU)	clientAuth, Code signing	Defines allowed certificate purposes.
Signature Hash Algorithm	SHA-256	

4. Certificate Policy Parameters

Parameter	Purpose
Basic Constraints	CA: False
Path Length Constraint	For intermediate CAs.
CRL Distribution Points (CDP)	http://cdp.TestOrg.gov.il/crl
Authority Information Access (AIA)	CA-TestOrg.
Certificate Policies (OID)	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.3
OCSP Must-Staple	False

5. Validity Parameters

Parameter	Notes
Requested expiration	3 years. Public TLS max is 397 days.
Start date	Actual Date
Renewal requirements	Automated via ACME or scripts.

6. CSR Attributes

Generate a **CSR (Certificate Signing Request)** with:

1.Subject DN
2.SAN list
3.Public key
4.Key size/curve

Verify and issue the certificate using the CSR.

7. Operational Metadata for the System

Metadata	Example / Purpose
System name / service name	"NTN"
Environment	Dev
Contact person	Israel Israeli (System Security Responsible Person)
NTN	NTN Local Host, Data Sharing Local Host
Private key storage	Local file, Secrets Manager
Automation requirements	ACME

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: MOH ,PCM**
- **קבלת הטוקן מנותן השירות ואישורו מול ה PCM (8)**
- **שליחת המידע לנותן השירות (9)**

נותן שירות

- קבלת קובץ עם תעודות הארגונים והטמעה בתשתית MTLS
- רישום בקשת הסכמה (1)
- תשאול לגבי הסכמה: סטאטוס, תוקף, מקורות מידע (6)
- קבלת טוקנים מה PCM לפנייה למקורות המידע (7)

הפגישות הבאות

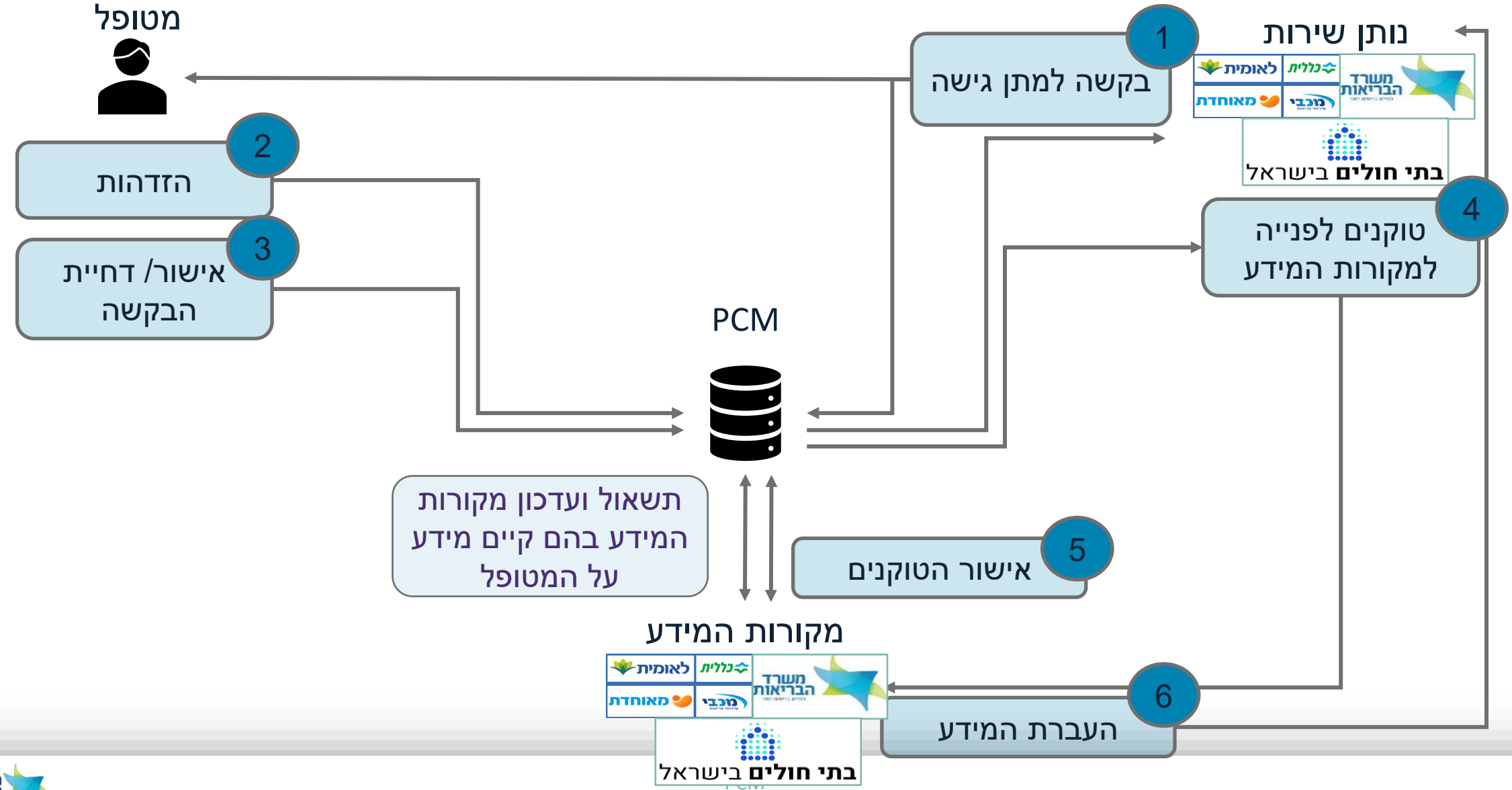
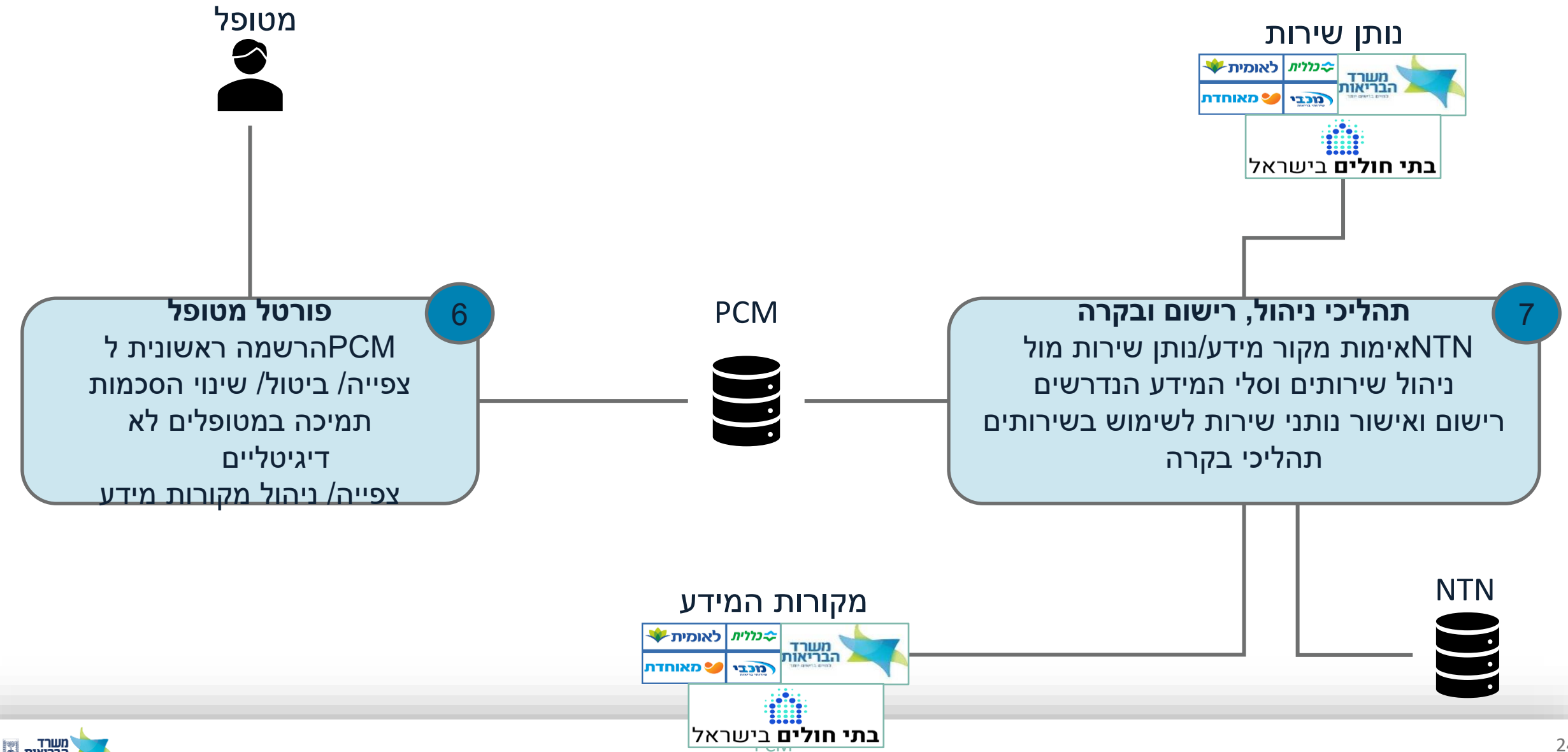
- DR ממשק נותן שירות MVP1 – 15.1.26
- אפיון תהליך הזדהות מול הקופות וקבלת מידע על חוסים – 8.1.26
- התנעת אינטגרציה לתכולות MVP1 – 24.3.26

FHIR® IL by 8400

משרד הבריאות
לחיים בריאים יותר

תודה רבה!

שחקנים ותהליכים מרכזיים



שחקנים ותהליכים מרכזיים