Sharing M3 content with Partners

Overview

Approach

The proposal is to utilise the Oauth 2.0 standard to share specific pieces of M3 content with members of a partner community in a way that is secure and enables M3 to accurately track engagement.

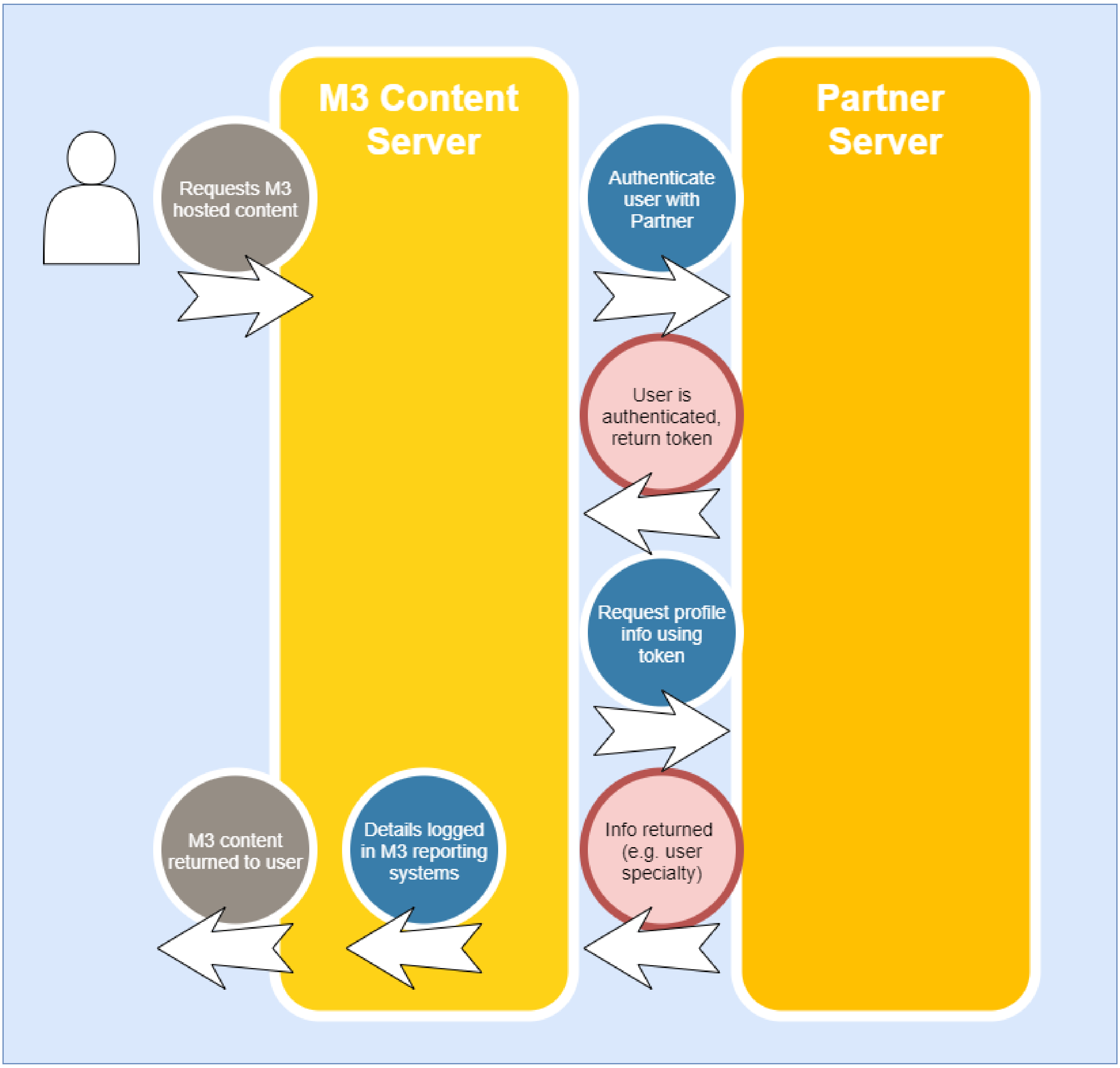
Principles of this approach:

- Partner members do not need to register with M3
- Partner members will only have access to specific agreed pieces of content, they are not granted access to M3 websites as a whole
- Agreed set of member profile information is shared with M3 for reporting purposes only, but never enough to personally identify a user

Simplified Overview of Flow

Detailed documentation of the Oauth flow and work needed to implement it can be found later in this document, but the below gives a simplified view of the flow.

If the partner member is already logged into the partner site the flow below will be invisible to the user and happen "behind the scenes". If not already logged in the member will be interrupted with the partner site login form after the first step.

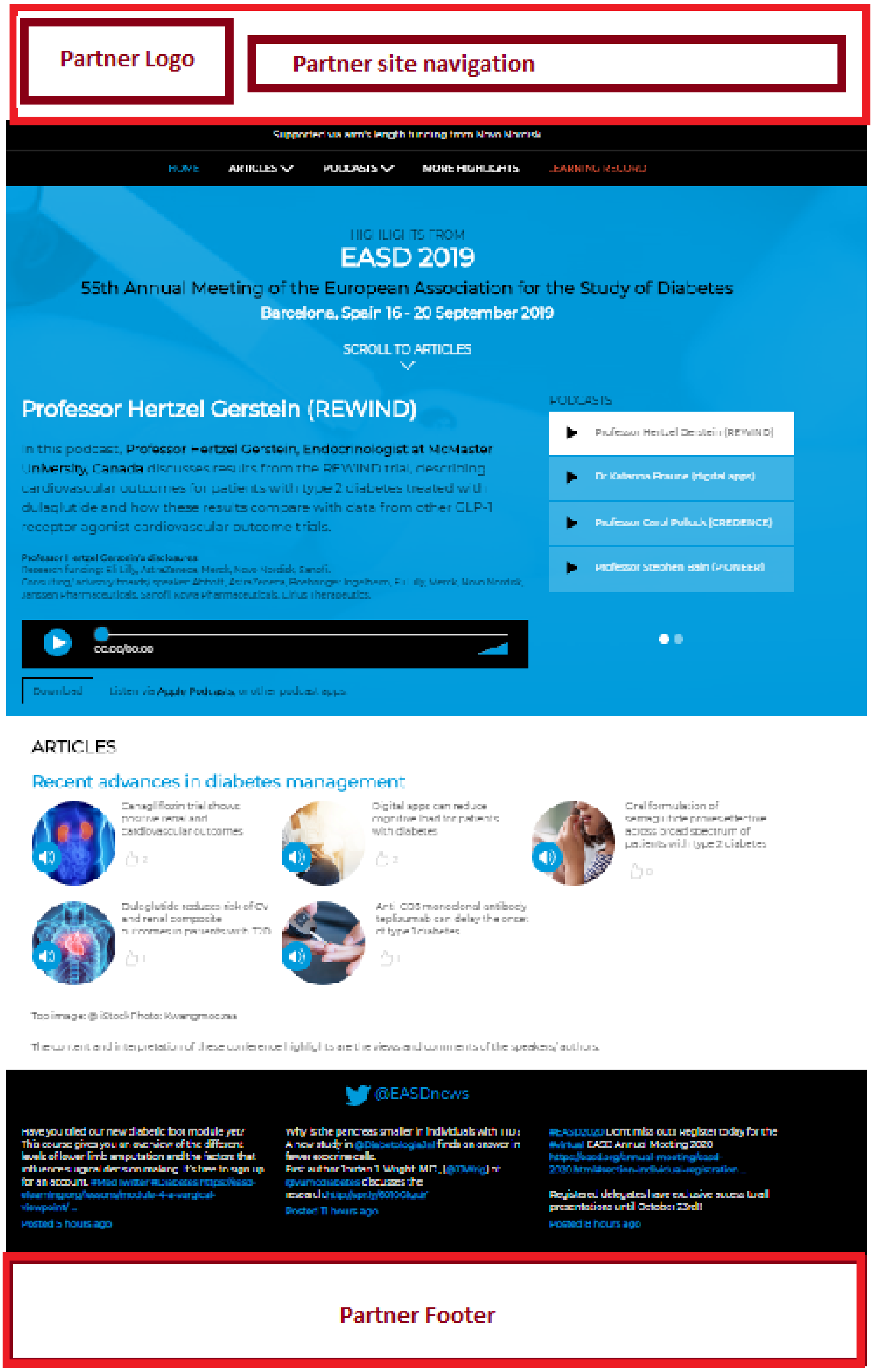

M3 Content Server
Partner Server
Requests M3 hosted content
Authenticate user with Partner
User is authenticated, return token
Request profile info using token
Info returned (e.g. user specialty)
Details logged in M3 reporting systems
M3 content returned to user

Header/Footer (optional)

There is the option of wrapping the M3 content inside a partner header and footer. This gives the user the impression that they are moving to another area of the partner's site. To acheive this M3 requires the partner to provide separate API endpoints which return the HTML of the header or the footer as requested.

This also provides the member a means to get back to the partner website.

If the partner header/footer is static, i.e. has no personalisation and is the same for all members, the HTML can simply be provided to M3 by the partner prior to content being published (no API endpoints needed).



Partner Logo

Partner site navigation

Supported via arm's length funding from Novo Nordisk

HOME ARTICLES PODCASTS MORE HIGHLIGHTS LEARNING RECORD

HIGHLIGHTS FROM

EASD 2019

55th Annual Meeting of the European Association for the Study of Diabetes

Barcelona, Spain 16 - 20 September 2019

SCROLL TO ARTICLES

Professor Hertzel Gerstein (REWIND)

In this podcast, Professor Hertzel Gerstein, Endocrinologist at McMaster University, Canada discusses results from the REWIND trial, describing cardiovascular outcomes for patients with type 2 diabetes treated with dulaglutide and how these results compare with data from other GLP-1 receptor agonist cardiovascular outcome trials.

Professor Hertzel Gerstein's disclosures
Research funding: Eli Lilly, AstraZeneca, Merck, Novo Nordisk, Sanofi.
Consulting/advisory boards/speaker: Abbott, AstraZeneca, Boehringer Ingelheim, Eli Lilly, Merck, Novo Nordisk, Janssen Pharmaceuticals, Sanofi, Kowa Pharmaceuticals, Cirius Therapeutics.

00:00/00:00

Download Listen via Apple Podcasts, or other podcast apps

PODCASTS

- Professor Hertzel Gerstein (REWIND)
- Dr Katerina Braune (digital apps)
- Professor Carol Pollock (CREDENCE)
- Professor Stephen Bain (PIONEER)

ARTICLES

Recent advances in diabetes management

Canagliflozin trial shows positive renal and cardiovascular outcomes 2

Digital apps can reduce cognitive load for patients with diabetes 2

Oral formulation of semaglutide proves effective across broad spectrum of patients with type 2 diabetes 0

Dulaglutide reduces risk of CV and renal composite outcomes in patients with T2D 1

Anti-CD3 monoclonal antibody teplizumab can delay the onset of type 1 diabetes 1

Top image: © iStockPhoto: Kwangmoozaa

The content and interpretation of these conference highlights are the views and comments of the speakers/authors.

@EASDnews

Have you tried our new diabetic foot module yet? This course gives you an overview of the different levels of lower limb amputation and the factors that influence surgical decision making. It's free to sign up for an account. #MedTwitter #Diabetes https://easd-elearning.org/lessons/module-4-a-surgical-viewpoint/ …
Posted 5 hours ago

Why is the pancreas smaller in individuals with T1D? A new study in @DiabetologiaJnl finds an answer in fewer exocrine cells. First author Thomas T Wright MD, (@TWrig) of @vumcdiabetes discusses the research https://buff.ly/3010Guur
Posted 11 hours ago

#EASD2020 Don't miss out! Register today for the #virtual EASD Annual Meeting 2020 https://easd.org/annual-meeting/easd-2020.html#section-individual-registration …

Registered delegates have exclusive access to all presentations until October 23rd!!
Posted 8 hours ago

Partner Footer

Reporting

As a minimum M3 will report on total engagement (impressions and clicks) and unique member engagement, and the only requirement for this to be possible is for a unique ID to be sent for each member as part of the Oauth flow.

For more detailed reporting M3 requires extra information to be passed, these are known as "scopes". The below defines typical scopes that can be used:

Scope	Description

Scope	Description
`User ID`	A unique ID per user, may be a string or number
`Specialty`	The user's medical specialty
`Seniority`	The user's medical seniority
`Country`	
`Doctor`	True or False. Useful for distinguishing staff/test accounts for example
`Groups`	This allows an arbitary list of tags to be assigned to a user. Can be useful if custom reporting is required that can't be satisfied by the above, for example by age groups

It is important that whatever info is transfered isn't enough to personally identify anyone. For example if postcode was passed in groups this may be fine on it's own, but in combination with user specialty it may become enough to find someone's identity.

Technical Implementation

Introduction

Authentication is handled using the OAuth 2.0 specification. OAuth is an open standard designed to enable users to authenticate themselves on site A using their existing account on site B. This is ideal for the scenario of sharing M3's content with partner communities.

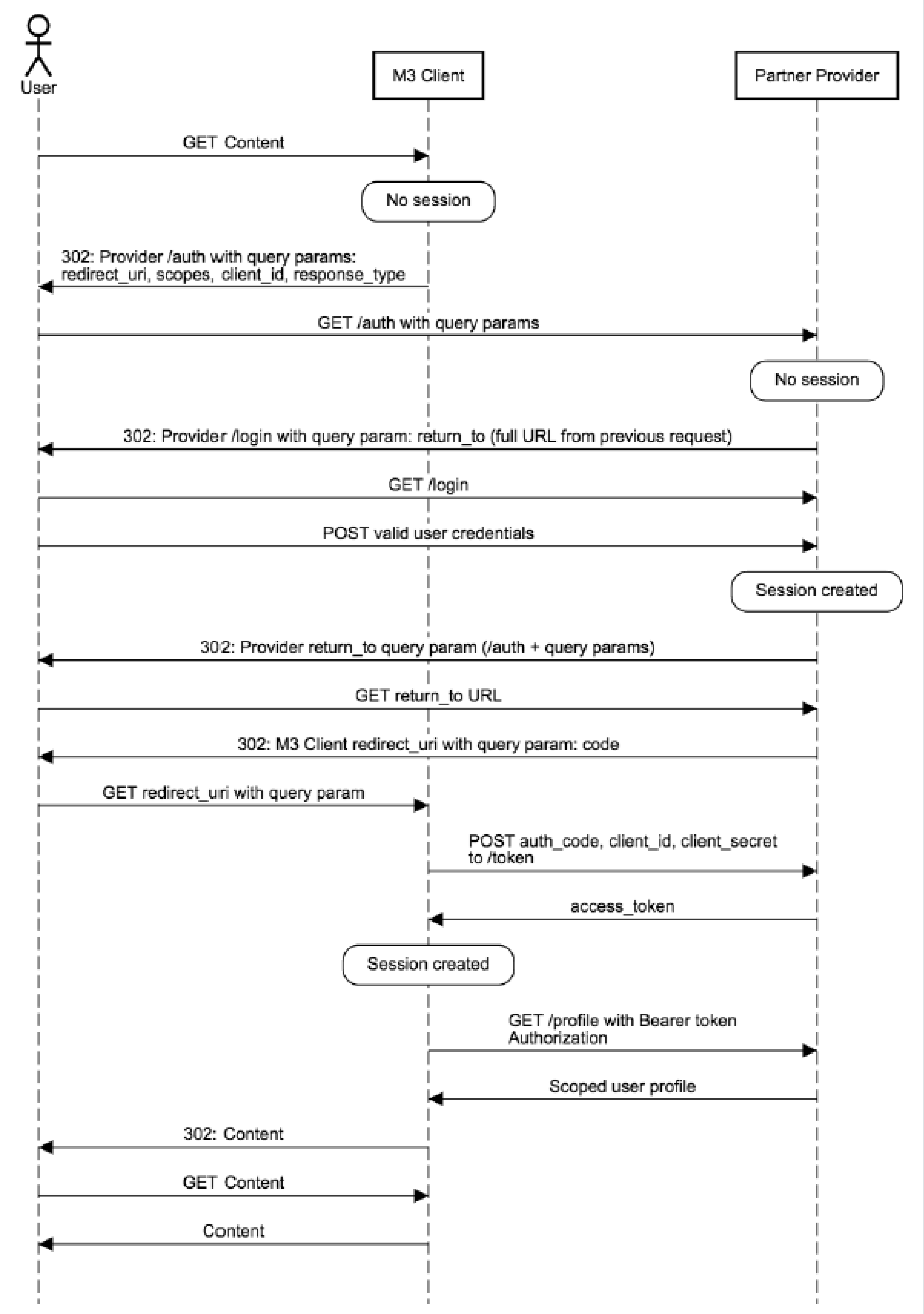
The OAuth authentication flow uses a number of user-agent redirects, passing data using query parameters and a server-to-server request to establish a login session. Visualising the flow can be difficult, so below is a sequence diagram showing the full flow of a non-logged-in user landing on M3 content for the first time.

OAuth Authentication Flow

We will first consider the case where a user arrives without a session on the client. The steps required to establish a session on the M3 Client can be summarised by the following points:

1. Create a cookie-based session on the partner OAuth provider.
2. Pass an auth_code to the M3 OAuth Client from the Partner Provider via user-agent redirect.
3. Make a server-to-server request from the M3 OAuth Client to the provider to exchange the auth_code for an access_token .
4. Make a server-to-server request from the M3 OAuth Client to the provider to get the user profile using the access_token .
5. Create a cookie-based session on the M3 Client.

Figure 1: Basic OAuth authentication flow for a not-logged-in user.


User
M3 Client
Partner Provider
GET Content
No session
302: Provider /auth with query params: redirect_uri, scopes, client_id, response_type
GET /auth with query params
No session
302: Provider /login with query param: return_to (full URL from previous request)
GET /login
POST valid user credentials
Session created
302: Provider return_to query param (/auth + query params)
GET return_to URL
302: M3 Client redirect_uri with query param: code
GET redirect_uri with query param
POST auth_code, client_id, client_secret to /token
access_token
Session created
GET /profile with Bearer token Authorization
Scoped user profile
302: Content
GET Content
Content

API Specification

To enable all of the above the Partner needs to implement the following API endpoints:

Method	Url	Description
`GET`	`/oauth/auth`	If the M3 client finds that the user has no valid session, then it will redirect the user to the PP Authorise endpoint.
`POST`	`/oauth/token`	After the PP has redirected the user to the M3OC callback endpoint, a server-to-server request will be made to exchange the provided auth_code for a valid access_token . The POST body will be sent with form encoding.
`GET`	`/oauth/profile`	Returns scoped profile information
`GET`	`/api/header`	(OPTIONAL) Serves the site header as a snippet of HTML that can be inserted into any page
`GET`	`/api/footer`	(OPTIONAL) Serves the site header as a snippet of HTML that can be inserted into any page