EMR EHR Connectivity 2.1

ONE Access Gateway – Business View

July 13, 2020

Document Version & Status: 1.1 – DFC (Draft for Comment)

Table of Contents

1. INTRODUCTION 3

1.1 OVERVIEW 3

1.1.1 What is the ONE Access Gateway? 3

1.1.2 What is Open Authorization 2.0? 3

2. SYSTEM VIEW 4

2.1 ONE ACCESS GATEWAY INTERACTIONS 4

2.2 ONE ACCESS GATEWAY PARAMETERS 5

3. APPENDIX A: GLOSSARY OF KEY TERMS AND DEFINITIONS 6

3.1 ACRONYMS AND ABBREVIATIONS 6

3.2 DEFINITIONS 7

1. INTRODUCTION

1.1 Overview

The Ontario Health (Digital Services) ONE Access Gateway (OAG) is a modernized platform for enabling the integration of client applications (e.g., EMR Offerings) with provincial clinical repositories and registries securely and reliably. It is a solution to better support the client applications to access EHR data through following a standards-based approach. All EHR products and services hosted on the OAG support Open Authorization 2.0 (OAuth2) and OpenID Connect (OIDC) for authentication and authorization.

1.1.1 What is the ONE Access Gateway?

The OAG enables client applications (e.g., EMR Offerings) to connect to and access EHR products and services using a standards-based approach to access data with flexibility and ease of use for developing solutions utilizing the HL7 FHIR standard.

1.1.2 What is Open Authorization 2.0?

OAuth2 with OIDC as the identity layer is an authorization framework utilized by the OAG to authenticate and authorize the client applications (e.g., EMR Offerings) and their users' access to various EHR products and services available.

2. SYSTEM VIEW

2.1 ONE Access Gateway Interactions

The following diagram provides a high-level overview of the role of the OAG, which acts as the protected resource for client applications (i.e., consumers) wishing to access EHR assets.

The API gateway will:

1. Accept and validate bearer tokens
2. Validate that signature from the token is from the ONE ID OIDC/OAuth2 service
3. Accept tokens that are active and not expired from the ONE ID OIDC/OAuth2 service
4. Check the audience claim to ensure that it includes the API OAG Identifier
5. Ensure the token has valid scope and profiles set to access the EHR Service
6. Call Line of Business (LoB) - Interpret Access Tokens using JSON web token (JWT)

Figure 1 – EMR Offering Interaction with the ONE Access Gateway to connect to an EHR product or service

2.2 ONE Access Gateway Parameters

The following table outlines the message header information that an EMR Offering needs to provide to authenticate and connect to the OAG.

ID	NAME	DEFINITION
1	X-Gtwy-Client-Id	The Gateway Client ID uniquely identifies each EMR tenant that is registered to connect to the OAG. It is assigned to each EMR tenant during the Ontario Health Digital Services registration process and is used to identify registered EMR tenants.
2	X-Gtwy-Client-Secret	The Gateway Client Secret is used to provision the EMR tenant for token creation. It is assigned to each EMR tenant during the Ontario Health Digital Services registration process. And is used to authenticate registered EMR tenant.
3	X-Request-Id	The Client Transaction ID is generated by the EMR Offering to uniquely identify each message sent by the EMR Offering and interacting with the OAG. The OAG will respond with a corresponding Gateway Transaction ID, to be used for troubleshooting, logging, and auditing purposes between the two systems (and also the EHR service).
4	X-LobTxId	The Line of Business ID uniquely identifies each EHR service. It will be provided by the OAG and may be required to be provided back by the EMR Offering to identify which EHR service the message or transaction relates to. For example, the EHR Service ID is used when setting the patient context to identify which EHR service is to use that patient context.

3. APPENDIX A: GLOSSARY OF KEY TERMS AND DEFINITIONS

3.1 Acronyms and Abbreviations

This table identifies definitions for terms used within or that are relevant to this document.

ACRONYM	DEFINITION
API	Application Programming Interface
DHDR	Digital Health Drug Repository
DHIR	Digital Health Immunizations Repository
EHR	Electronic Health Record
EMR	Electronic Medical Record
FHIR	Fast Healthcare Interoperability Resources
HIC	Health Information Custodian
HL7	Health Level Seven
IETF	Internet Engineering Task Force
JSON	JavaScript Object Notation
JWT	JSON web token
LoB	Line of business
OAG	ONE Access Gateway
OAuth2	Open Authentication 2.0
OHDS	Ontario Health (Digital Services) - formerly eHealth Ontario
OIDC	OpenID Connect
OIDF	The OpenID Foundation
PEM	Privacy Enhanced Mail
ReST	Representational State Transfer
SSO	Single Sign-On
UAO	Under the Authority of
URI	Uniform Resource Identifier

ACRONYM	DEFINITION
URL	Uniform Resource Locator

3.2 Definitions

The following are the terms and definitions used to describe the concepts used in this document.

TERM	DEFINITION
EMR tenant	A tenant applies to an EMR used by an individual or a group of people. For example, a tenant could be a single-family physician or a family health team comprised of many EMR users and distributed across several clinics.
EMR user	A user who has access rights to log into an EMR. This can be an end-user, an administrative user who administers the EMR, or any other user of the EMR. They may or may not also have access to an EHR service.
EHR user	A user who has access rights to one or more EHR services. Typically, an EHR user is also an EMR user.
Gateway Client ID	The Gateway Client ID is the information assigned as part of an Ontario Health Digital Services process to register an EMR Offering instance to allow it to connect to the OAG as part of the OAuth2 interaction. It uniquely identifies the EMR Offering instance and is provided by the EMR as part of the interaction when connecting to the OAG.
Gateway Client Secret	The Gateway Client Secret is a private key used to authenticate a registered EMR Offering to connect to the OAG. It should be kept confidential and stored securely.
Gateway endpoint	This is the URL for the EMR Offering to connect to the OAG. This value will be different for differing environments (e.g., a test vs. production environment).
PEM	It is a Base-64 encoded X.509 certificate. In the context of the OAG, it is used to validate the signature of a JWT.
Under the Authority of (UAO)	This information defines the HIC or organization of which an EMR user is authorized to act on behalf. Because a HIC or organization can be represented by a single physician, or an organization consisting of multiple physicians, the UAO can be tied to an EHR user account as well as a Client ID that represents an EMR system. The UAO is assigned by Ontario Health (Digital Services)as part of a registration process for the EHR user to receive their ONE ID account, and to register an EMR system to represent the HIC or organization. An EMR user and/or a clinic may be assigned zero, one, or multiple UAO values. A user or clinic who has not completed registration, or who does not belong to an organization

TERM	DEFINITION
	would not be assigned a UAO. An EMR user who works at a single organization, or a clinical practice that operates under a single organization would be assigned one UAO, and a user or clinic practice that functions under multiple organizations would be assigned multiple UAO values respectively. Multiple EMR Offering instances or users working for the same organization would be assigned the same UAO. An EHR service, depending on its function, may rely on the UAO of the EMR user (where access is user-based), or the UAO of the clinic (if it is system-based), or a combination of them. As a result, an EMR Offering instance needs to be assigned at least one UAO to connect to the OAG. Similarly, an EMR user needs to be assigned at least one UAO to access an EHR service hosted on the OAG.