EMR EHR Connectivity

ONE Access Gateway – Business View

May 21, 2021

Document Version & Status: 2.1 – DFU (Draft for Use)

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 (OHDS) ONE Access Gateway (OAG) is a modernized platform enabling the integration of client applications, such as EMR Offerings, with provincial clinical repositories and registries. It supports client applications by providing access to EHR data following a standards-based approach. EHR products and services hosted on the OAG support Open Authorization 2.0 (OAuth2) and OpenID Connect (OIDC) for authentication and authorization to enable secure and reliable transactions.

1.1.1 What is the ONE Access Gateway?

The OAG enables 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. It is the gateway that hosts and provides access to multiple EHR products and services that follow the same connectivity standard, where historically, different EHR products and services each followed different standards to connect, authenticate and authorize EMR users to those assets.The OAG enables a standardized approach for authentication and authorization, minimizing the need for EMR developers to adopt and develop to multiple standards.

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 an EMR Offering wishing to access EHR products or services.

The OAG 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 product or service
6. Call EHR Service - 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 information that an EMR Offering needs to provide in order to authenticate and connect to the OAG. Further implementation details for EMR Offerings and other types of client applications are available in the OHDS "ONE Access Gateway - Transport Specification".

ID	NAME	VALUE ASSIGNED BY	DEFINITION
1	X-Gtwy-Client-Id	OHDS	The Gateway Client ID uniquely identifies each EMR tenant that is registered to connect to the OAG. This value is assigned to each EMR tenant during the OHDS registration process and is used to identify registered EMR tenants.
2	X-Gtwy-Client-Secret	OHDS	The Gateway Client Secret is used to provision the EMR tenant for token creation. This value is assigned to each EMR tenant during the OHDS registration process and is used to authenticate registered EMR tenant.
3	X-Request-Id	EMR Offering	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. This value aids to correlate transactions logged by the EMR Offering with transactions logged by 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	OHDS	The Line of Business ID uniquely identifies each EHR service available on the OAG. This value is assigned to each EHR Service during the OHDS registration process for each EHR Service. EMR Offerings can this number to refer to the specific 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
HEART	Health Relationship Trust Profile (for OAuth 2.0)
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 (EHR product or service)
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

ACRONYM	DEFINITION
URI	Uniform Resource Identifier
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	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 set of data uniquely identifies the Health Information Custodian (HIC) or organization that an EMR user is authorized to act on behalf. The UAO is assigned as part of the OHDS registration process for each HIC. The relationship between the HIC and a clinician is tied to the EMR user's ONE ID account, and can also be tied to that user's EMR account in the EMR Offering.

TERM	DEFINITION
	Because an EMR user may act on behalf of one or more HICs, an EMR user's may possibly be related to one or more UAOs. (It may also have zero UAO values tied to it if the EMR user has not registered with OHDS for a ONE ID account.)