Federated authentication and Web Single Sign-on mandatory Requirements

Acronyms

HIS – Health Information System/s

IDP – Identity Provider

SP – Service Provider

ADFS – Active Directory Federation Services

SAML – Security Assertion Markup Language

GPA IDP – Government Public Administration IDP

Background

All Health Information Systems (HIS) need to speak common authentication language, and all user credentials are stored and managed by a common identity provider (IDP). Furthermore all web based systems need to provide a single sign-on experience to the end users, whereby a user will be able to authenticate once and seamlessly access all web based systems within the same single sign-on ecosystem. It is therefore important that all new procurements implement a federated authentication mechanism and a web single sign-on profile. Currently the federated identity provider for government is the Government Public Administration IDP (GPA IDP).

SAML 2.0 WebSSO

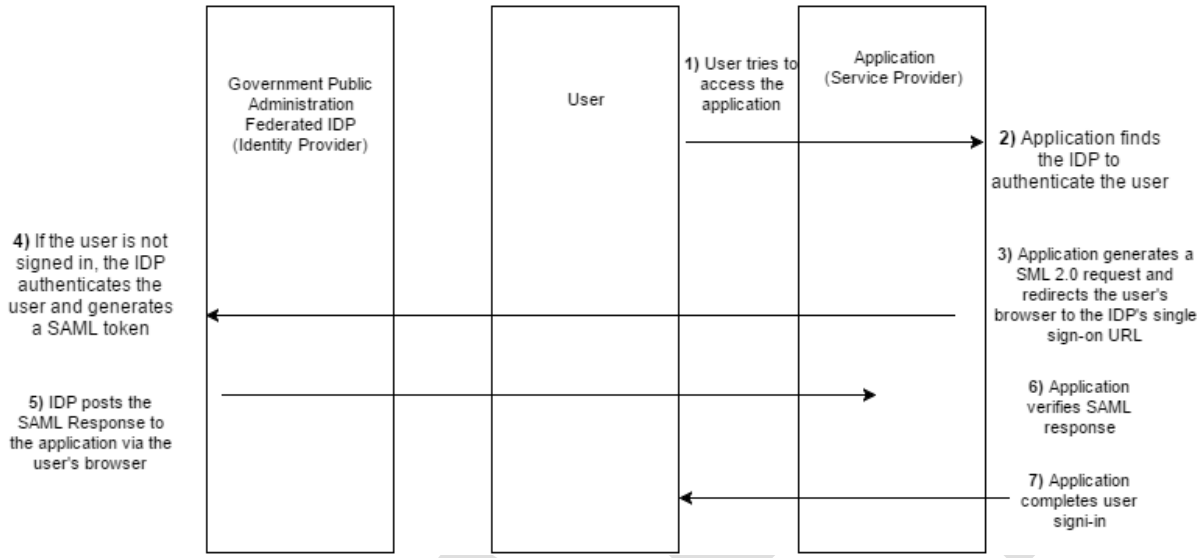
SAML 2.0 is the protocol chosen to achieve web SSO in the HIS.

Security Assertion Markup Language, otherwise known as SAML, is an XML-based open standards for exchanging authentication and attributes (claims) between an identity provider and a service provider (website). At its core, SAML is a series of XML-based messages that detail whether a person has authenticated, and frequently information about that person

In web single sign-on, a user authenticates to one web site and then, without additional authentication, is able to access some personalized or customized resources at another site. SAML enables web SSO through the communication of an authentication assertion from the first site to the second which, if confident of the origin of the assertion, can choose to log in the user as if they had authenticated directly.

What basically happens is that IDP and SP exchange SAML protocol messages through the user's browser. The SP sends an SAML authentication request message to the IDP, asking to authenticate the user. The IDP typically asks the user for a username and password (although any other method of authentication can be used) and if the password is correct, the IDP sends back a SAML

authentication response stating that the user has just logged in successfully at the IDP, together with some proof that the message was indeed sent by the IDP.



High level SAML 2.0 Web SSO Flow

Federated Identity and WebSSO mandatory requirements for prospective providers of HIS to GOM

The bidder (service provider) confirms that it adheres and/or is able to deliver the requirements described.	Requirement	Description
Yes/No	Adheres to guidelines on service provider integration with Government Publc Administration (GPA) IDP	Understand and adhere to detailed specifications as provided in http://bit.ly/1SZRleA
Support and implement the SAML 2.0 conformance and operational modes (relevant for Identity Provider Lite and Service Provider Lite operational modes) listed below in line with the Web Browser SSO profile as defined in the GPA Federated Authentication Guidelines		

http://bit.ly/1SZRleA :	
	Functions
Yes/No	Web SSO, <AuthnRequest>, HTTP Redirect
Yes/No	Web SSO, <Response>, HTTP POST
Yes/No	Web SSO, <Response> , HTTP Artifact
Yes/No	Artifact Resolution, SOAP
Yes/No	Single Logout (IdP-initiated) - HTTP Redirect
Yes/No	Single Logout (SP-initiated) - HTTP Redirect