

GLS Application Integration Overview

Overview

The GLS is a major component of the State Services Commission's All-of-government Authentication Programme (Authentication Programme).

Agencies who wish to integrate their online services (through their web applications) with the GLS must introduce a limited number of software components within their Internet application environment.

The GLS uses SAML (Security Assertion Markup Language) to facilitate the communication to the agency of security assertions regarding a successful user logon at the GLS. An agency is required to have a SAML component in addition to or built into their online application to facilitate secure messages.

Open standards for security based messaging services

In the past, there have been several open standards that have been adopted globally. The three major ones were [SAML version 1.1](#) (Security Assertion Markup Language) from [OASIS](#), [Liberty Alliance's Identity Federation Framework \(ID-FF\) v1.2](#), and [Shibboleth](#). All three of these have come together in SAML [version 2.0](#) (SAML2.0).

In 2008, SAML2.0 has become sufficiently mature for the GLS to implement.

SAML Solution

The Authentication Programme team provides consultation and advice on the appropriate SAML version (1.1. or 2.0) and topology for an agency's SAML component as part of adopting the GLS.

There are a number of benefits to agencies in choosing SAML2.0 such as;

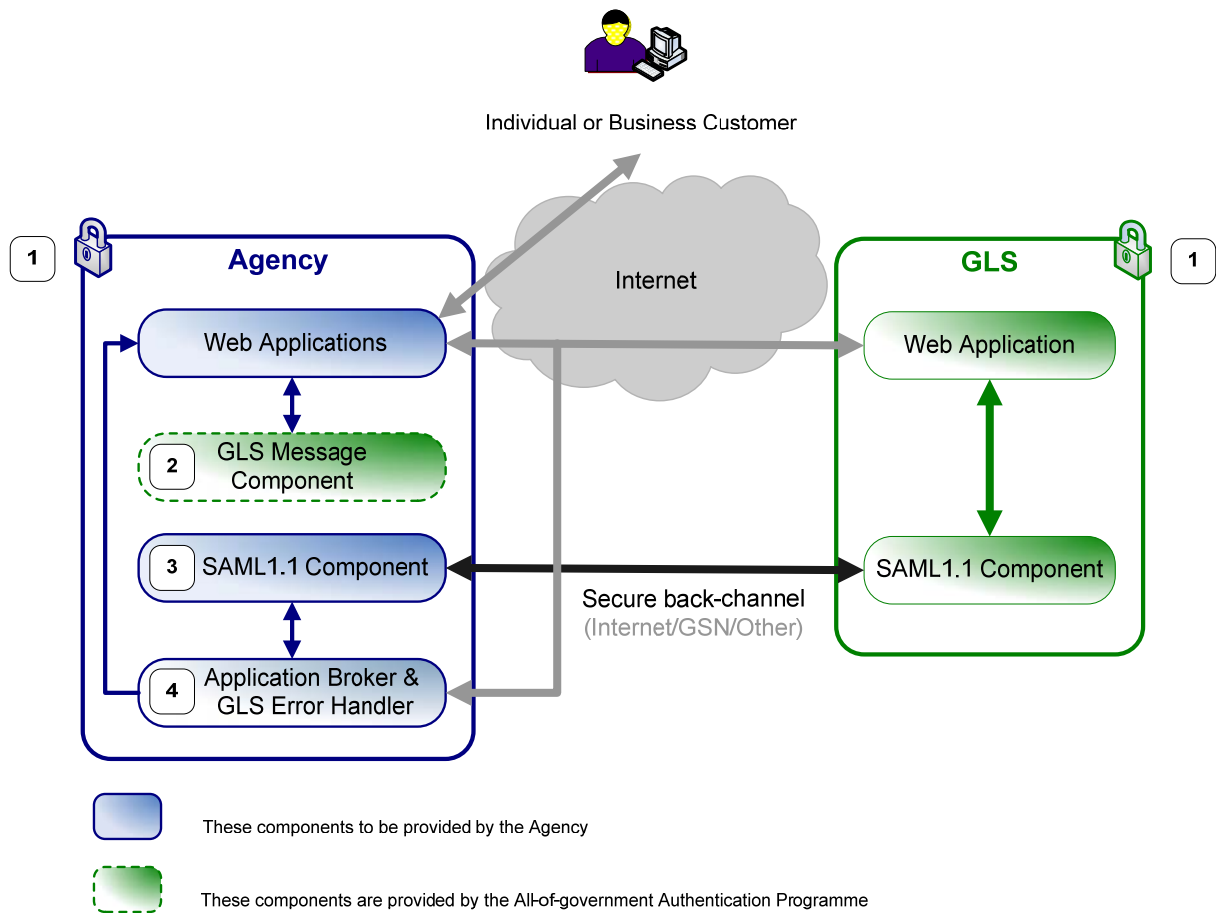
- it enables greater use of open standards for security-based messaging thereby removing the need for custom messages in GLS
- it supersedes SAML1.1 and the majority of new SAML vendor products target SAML2.0 messaging only
- the NZ Government Identity Verification Service (IVS), intended for release in 2009, will use SAML2.0 and thus an agency integrating against the GLS using SAML2.0 will have the appropriate technology in place for future use of the IVS
- any future support introduced into the GLS for Single Sign On will be via SAML 2.0 only

Agencies that have currently integrated using SAML1.1 together with custom messages will continue to be supported until all existing participating agencies have implemented to SAML 2.0.

The following diagrams for SAML1.1 and SAML2.0 depict the main integration components required to integrate an agency's online service with the GLS solution. A brief overview of each of these components is also provided. Please note that the diagrams are not intended to detail data flows or the various messaging scenarios.

SAML1.1 Solution

Agency and GLS - Integration Component View
Custom GLS Messaging and SAML1.1



SAML1.1 Integration Components

1. Security

Security in the system is facilitated through the use of digital certificates within the GLS and an agency's own environment. In the SAML1.1 solution digital certificates are used for encryption of custom and SAML messaging, mutual authentication between the GLS and the agency servers on the SAML back-channel and for digital signatures within SAML messages.

2. GLS Message Component

To interact with the GLS, an agency's web application must send specifically formatted messages to initiate a logon or creation of a new user account request.

A fully detailed message specification exists to support this operation although for most environments the Authentication Programme is able to provide a software library to simplify the message creation and thus ease the integration steps with the GLS.

3. Agency SAML1.1 Component

The GLS uses SAML1.1 to facilitate the communication to the agency of security assertions regarding a successful user logon at the GLS. The agency's SAML1.1 component isolates this message interaction from the agency's application(s).

There are two options an agency has for the topology of a SAML1.1 component within their infrastructure, namely:

1. A component embedded within a web application integrated with the GLS.
2. A centralised component resident within the agency's enterprise.

In general a SAML1.1 component embedded within a web application is only suitable, from an architectural standpoint, for agencies that want to enable authentication with the GLS of users with one web application only. If more than one web application will be integrating with the GLS within the same agency environment then it is recommended a centralised SAML1.1 component be adopted.

Agencies have various options for how to introduce a SAML1.1 component into their environment; these range from in-house coding, utilising a third party library, open source software or procuring a commercial SAML1.1 product.

4. Application Broker and GLS Error Handler

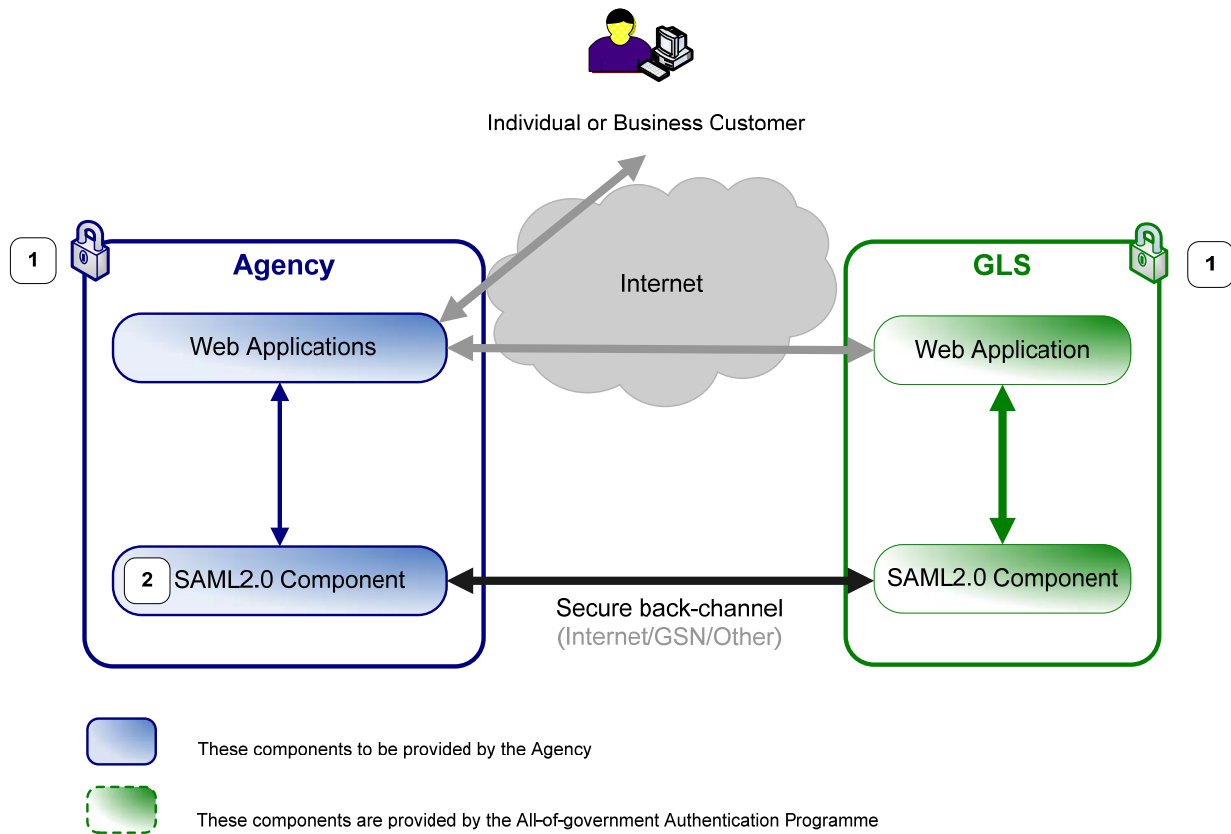
If a centralised SAML1.1 component is used by the agency, as discussed previously, an application broker may be required to propagate successful GLS logon details to the relevant application (that initiated the logon with the GLS). The Authentication Programme is able to offer consultation with regard to options for establishing such an application broker.

In addition to any required application broker, all agencies require a single GLS error handler. In the event of any errors, or user termination of logon, an error message will be sent to the agency where those details must be captured and integrated into the page flow of the application associated with the error.

Much like the application broker component (if applicable to the agency), details of the specific application associated with the error message from GLS is included in the error details to ensure propagation of the information in question is easily brokered to the relevant application.

SAML2.0 Solution

Agency and GLS - Integration Component View SAML2.0



SAML 2.0 Integration Components

1. Security

Security in the system is facilitated through the use of digital certificates within the GLS and an agency's own environment. In the SAML2.0 solution digital certificates are used for encryption of SAML messaging, mutual authentication between the GLS and the agency servers on the SAML back-channel and for digital signatures of SAML messages.

2. Agency SAML2.0 Component

To initiate a logon at the GLS, and potentially to interact with other similar New Zealand government SAML2.0 based services in the future, an agency's web application must trigger the sending of a SAML2.0 authentication request message to the GLS; part of the functionality to be provided by the agency's SAML2.0 component is to create such a message.

In turn the GLS will provide the initiating agency with security assertions regarding a successful user logon. The agency's SAML2.0 component will provide the capability to consume this type of assertion and broker the details back to the initiating web application within the agency's enterprise.

In the event of any errors, or user termination of logon, an error message will be propagated from the GLS to the agency's SAML2.0 component where in turn it will be brokered to the initiating web application and integrated into the page flow of the application associated with the error.

The agency's SAML2.0 component isolates the agency's application(s) from the message interaction with the GLS.

There are two options an agency has for the topology of a SAML2.0 component within their infrastructure, namely:

1. A component embedded within a web application integrated with the GLS.
2. A centralised component resident within the agency's enterprise.

In general a SAML2.0 component embedded within a web application is only suitable, from an architectural standpoint, for agencies that want to enable authentication with the GLS of users with one web application only. If more than one web application will be integrating with the GLS within the same agency environment then it is recommended a centralised SAML2.0 component be adopted; such a component topology will need to support the brokering of assertion details and any errors back to the initiating web application within the agency's enterprise.

Agencies have various options for how to introduce a SAML2.0 component into their environment; these range from in-house coding, utilising a third party library, open source software or procuring a commercial SAML2.0 product.