Service Description – Enterprise Access

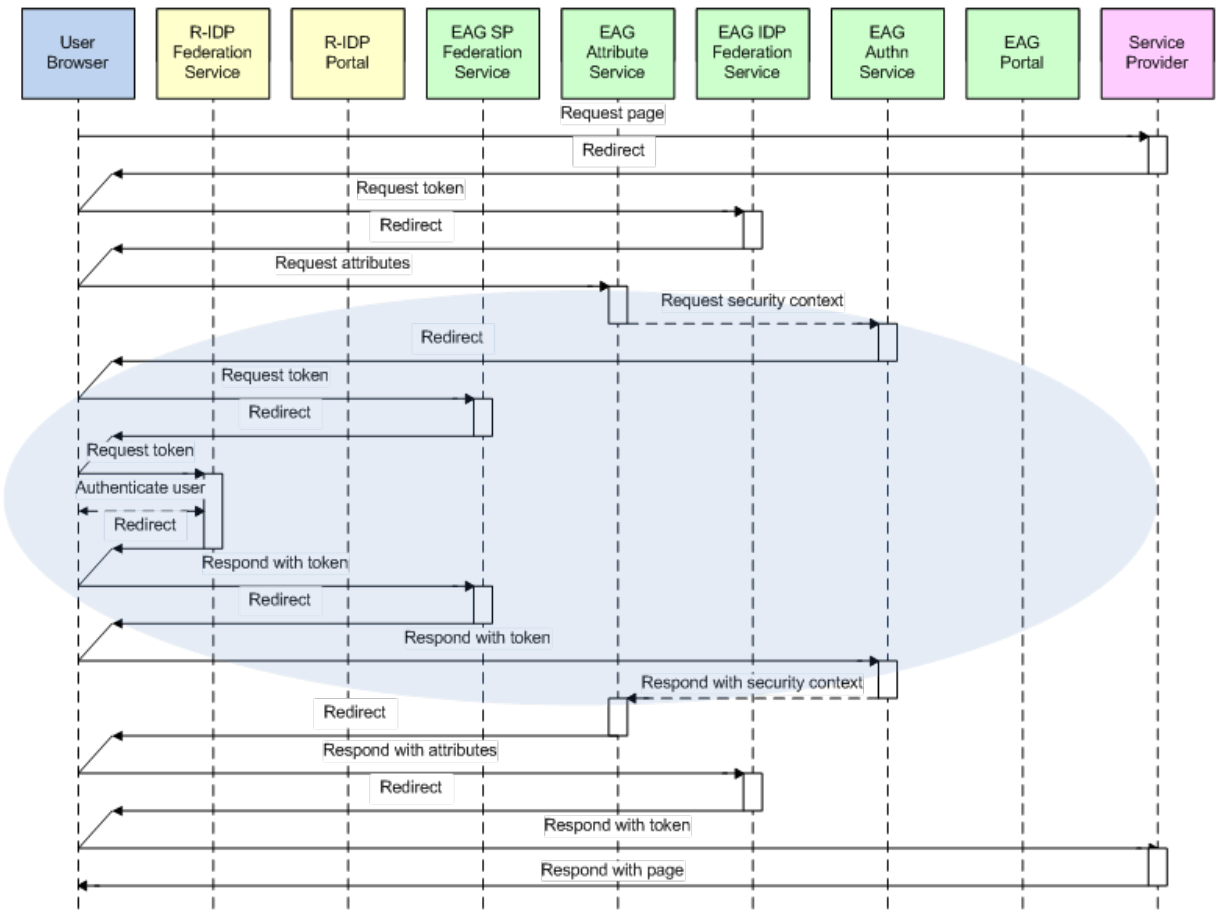
Gateway for Life Sciences

This section describes Exostar's Enterprise Access Gateway Service as it pertains to the integration of the Subscriber acting as a Remote Identity Provider ("R-IdP") and asserting user authentication information to Exostar and affiliate Service Providers ("SP").

The following describes what happens at runtime, when an R-IdP user attempts to access resources within Service Provider-hosted applications or Exostar's Secure Access Manager ("SAM"). ***Exhibit 1*** of this document outlines the requirements of an R-IdP integrating with Exostar's Enterprise Access Gateway ("EAG").

An end user may engage with EAG pointing their browser to the SP or to SAM. In the latter scenario, SAM acts as an SP. Regardless of the starting point, the browser shall be redirected to the R-IDP, which provides user attributes back to the Exostar Federation Service.

A federation assertion from an R-IDP shall meet the assertion format and protocol requirements in **Exhibit 2** of this document. The following illustrates the Exostar and R-IdP system flows during authentication:



The following illustrates the Exostar and R-IdP system exception handling during authentication:

Condition	Occurs	Description	Error Message
When presented with the EAG/SAM logon page, the user selects an R-IDP whereas in reality his IDP is SAM	At runtime	Will fail auth at R-IDP	Authentication errors occurring within the R-IDP systems will result in an authentication error as defined by the R-IDP. Authentication errors occurring within Exostar systems will result in a system generated message, "This page is displayed because you are not authorized to access this portion of the website. Please contact your system administrator for details."
When presented with the EAG/SAM logon page, the user selects an incorrect R-IDP	At runtime	Will fail auth at R-IDP	
When presented with the EAG/SAM logon page, the user chooses SAM whereas in reality his IDP is some R-IDP	At runtime	Will fail auth at SAM	
Incorrect realm name provided in the federation token by the R-IDP	At runtime or during account linking	Will fail login to SAM	
Incorrect/expired assertion-signing certificate from R-IDP	At runtime or during account linking	Will fail login to SAM	
Missing LoA and/or UK Restricted elements in the assertion from R-IDP	At runtime	Will fail login to SAM	
The user whose IDP is some R-IDP (e.g., Enterprise) fails to authenticate to that R-IDP when redirected to it by SAM. (Not applicable to the case of Integrated Windows Logon where the user is not challenged after initial authentication to his desktop.)	During account linking	No account linking occurs, must repeat	
The user whose IDP is some R-IDP (e.g., Enterprise) fails to authenticate to that R-IDP when redirected to it by SAM. (Not applicable to the case of Integrated Windows Logon where the user is not challenged after initial authentication to his desktop.)	At runtime	Will fail auth at R-IDP	
User failed to remove the IDP Cookie as instructed in the e-mail from SAM/EAG	During account de-linking	Will fail login to SAM. Note, user delinking is available only to Exostar customer support; therefore removal of the cookie must be user driven through a link provided by Exostar.	

Joint interoperability testing must be conducted between Exostar and the R-IdP prior to the enablement of production level connections to Exostar's systems. Appropriate resources within Exostar and the R-IdP shall be made available to complete testing before and at the time of Production enablement. Test and Production systems within the R-IdP (as outlined in **Exhibit 1** of this document) must be available to complete testing.

Primary test cases include the following, with Exostar signoff required:

1. R-IDP provides properly formatted assertion
2. The system to system flow outlined above will execute to fruition
3. Exceptions for error conditions are handled as defined above
4. Validation of successful login through EAG to an SP

The Subscriber (and the R-IDP) warrants, represents and agrees that all information in the attached security questionnaire (**Exhibit 3** attached hereto), completed by the R-IDP, is accurate and complete. The R-IDP further agrees that any significant changes to the R-IDP configuration will be documented in an updated security questionnaire, which will be provided to Exostar.

The Subscriber (and the R-IDP) agrees that Exostar may, and authorizes Exostar to, disclose the information provided in **Exhibit 3** with other Exostar services subscribers with which Subscriber engages in connection with the Services. Such sharing facilitates access of the Subscriber (and the R-IDP) to the customer applications connected to Exostar.

Exhibit 1

R-IdP Responsibilities

An R-IDP is solely responsible for the development and maintenance of the following top level components:

1. Creation of a Federation service, such that local, enterprise employee credentials may be properly formatted and asserted to Exostar as defined in this document.
    a. A user's asserted authentication strength is contractually bound to be accurate and in accordance with this Service Agreement.
2. Deploy enterprise access groups / roles that may be used to support the Federation service (Exostar Recommendation only)
3. Ensure federation service access (http) is publicly available to users
4. Build in redundancy and error reporting that is in alignment with your enterprise' corporate policies
5. Ensure there is sufficient audit logging such that individual enterprise login events and successful assertions can be reconstituted in the event of audit or dispute.

Unless otherwise agreed upon, the Identity Federation protocol shall be one of the following:

- WS-Federation, Passive Requestor Interoperability Profile (PRIP) using SAML 1.x assertions, or
- SAML 2.0, Web Browser SSO Profile

All communications between a user's Web browser, the R-IDP, and Exostar shall be over a server-authenticated SSL/TLS channel.

As required, Subscriber and Exostar will update interface specification to accommodate updates to technology and industry maturity levels. Updates will be documented and agreed upon in future versions of the EAG Service Agreement.

If Subscriber implements JIT provisioning, Subscriber will use Exostar's published specifications. All terms incorporated in this agreement will remain in force.

Exhibit 2

R-IdP Assertion Format and Protocol (v1.2)

Enterprise Access Gateway expects the attributes listed in the table below. If applicable, alternate Level of Authentication values are listed on the following page.

Profile	Claim	Description	Values	Value Description	Mandatory	Multi-valued
Std	specificationid	Unique ID of the specification the assertion adheres to	**Must** be set to urn:com:exostar:assertion-profiles:eag:1.1	Unique ID of the specification the assertion adheres to	Mandatory	
Std	subject	**Permanent** user identifier	Example: 25892e17-80f6-415f-9c65-7395632f0223 user12345@ad.lockheed.com	Asserted as the Subject	Mandatory	
Std	userprincipalname	User principal name (AD)	Example: 2001358769@mil	User principal name (AD)	Optional	
Std	assurancelevel	OMB 04-04 /NIST 800-63-1 identity assurance	level_1	OMB 04-04 Level of Assurance 1	Mandatory	
			level_2	OMB 04-04 Level of Assurance 2 (Password or Password + Basic Assurance Certificate)		
			level_3	OMB 04-04 Level of Assurance 3 (Medium Software + password)		
			level_4	OMB 04-04 Level of Assurance 4 (Medium Hardware Certificate + PIN)		
			unknown	The level is unknown		
Std	credentialsource1	The source or issuer of the authentication credential.	Example: exostar Example: merckridp	Mnemonic identifier of the remote Identity Provider/ Credential Provider	Mandatory	
Std	authenticator1	The entity authenticating the credential	Example: exostar Example: bae-greenlink	Mnemonic identifier of the party that authenticated the credential.	Mandatory	
Std	credentialtype1	The type of authentication credential Refer to SAML Authentication Context	password	Application account user-id and password	Mandatory	
			oob_otp	Out-of-band (phone) OTP		

		for starting list for this set of authenticators	sf_otp	OTP Token password		
			bloa_soft_cert	BLOA software based PKI credential (via SSL)		
			mloa_soft_cert	MLOA software based PKI credential (via SSL)		
			mf_otp	OTP Token password + activation factor		
			mloa_hard_cert	MLOA hardware based PKI credential (via SSL)		
			mob_otp	Software based OTP generated on a mobile device.		
			mob_push	Software based OTP delivered through mobile push notification.		
			unknown	The credential type is not known to the producer of this claim		
Std	credentialsource2	optional 2nd occurrence			Optional	
Std	authenticator2	optional 2nd occurrence			Optional	
Std	credentialtype2	optional 2nd occurrence			Optional	
Std	credentialsource3	optional 3rd occurrence			Optional	
Std	authenticator3	optional 3rd occurrence			Optional	
Std	credentialtype3	optional 3rd occurrence			Optional	
Std	uspersonstatus	User's US person status	us_person non_us_person unknown	Title 50 U.S.C. Not a US person US Person status not known for the subject (alternately, this attribute is absent)	Optional Default: unknown	

Std	sslprotocol	Version of the SSL protocol used at logon in a Passive Requester scenario	TLSv1.2 TLSv1.3	Note: TLSv1.1 is outdated. This attribute is named SSLProtocol for backwards compatibility reasons. The SSL protocol itself has been deprecated and is not used. Optional	Optional	
Std	businessrole	Business Role relevant for Business Application	Example: exostar:sam:restricted	A declared claim asserting that the User has explicit authorization to access MAG Restricted Profile	Optional If not present no roles will be assigned to the user.	Yes
				A claim identifying the business role of the user, which is relevant for the Business Application they are accessing		
Std	proofinglevel	User identity proofing level	level_1	No Vetting Process	Mandatory	
			level_2	Basic Vetting Process Such as e-mail address validation		
			level_3	Based on validation that OTP was shipped to the person and confirmation from an authorized party.		
			level_4	Face-to-face proofing		
			unknown	The level is unknown		

			mloa_soft_cert	MLOA software based PKI credential (via SSL)		
			mf_otp	OTP Token password + activation factor		
			mloa_hard_cert	MLOA hardware based PKI credential (via SSL)		
			unknown	The credential type is not known to the producer of this claim		
Std	credentialsource2	optional 2nd occurrence			Optional	
Std	authenticator2	optional 2nd occurrence			Optional	
Std	credentialtype2	optional 2nd occurrence			Optional	
Std	credentialsource3	optional 3rd occurrence			Optional	
Std	authenticator3	optional 3rd occurrence			Optional	
Std	credentialtype3	optional 3rd occurrence			Optional	
Std	uspersonstatus	User's US person status	us_person non_us_person unknown	Title 50 U.S.C. Not a US person US Person status not known for the subject (alternately, this attribute is absent)	Optional Default: unknown	
Std	sslprotocol	Version of the SSL protocol used at logon in a Passive Requester scenario	sslv2 sslv3 tlsv1	SSL 2.0 SSL 3.0 TLS 1.0 The conenction does not use SSL (alternately, this attribute is absent)	Optional default: sslv2	
Std	businessrole	Business Role relevant for Business Application	exostar:mag:restricted	A declared claim asserting that the User has explicit authorization to access SAM Restricted Profile	Optional If not present no roles will be	Yes

			Example: lmco:lmp2p:buyer lmco:lmp2p:corp_admin ADFSp2p.ap.accounts.payable.specialist ADFSp2p.r2p.buyer.sca ADFSp2p.xp.corporate.supplier.admin ADFSp2p.rp2.purchasing.manager ADFSp2p.xp.corporate.admin ADFSp2p.ap.pcard.administrator ADFSp2p.xp.display.user	A claim identifying the business role of the user, which is relevant for the Business Application they are accessing	assigned to the user.	
Std	proofinglevel	User identity proofing level	level_1	No Vetting Process	Mandatory	
			level_2	Basic Vetting Process Such as e-mail address validation		
			level_3	Based on validation that OTP was shipped to the person and confirmation from an authorized party.		
			level_4	Face-to-face proofing		
			unknown	The level is unknown		

1. Note that the R-IDP will assert the credential strength, including certificate authentication level (if applicable). However, in the scope of ForumPass which utilizes the certificates at runtime for encryption within “sensitive” sites, the certificates must be Exostar issued Basic Level of Assurance or Medium Level of Assurance (CertiPath compliant) certificates.

2. SSL Protocol – Note that TLSv1 is an authentication requirement for UK restricted access within ForumPass. The protocol utilized between the browser and R-IDP during authentication, or in this case, during the assertion generation should be captured and sent as part of this assertion. A recommendation may be to configure the R-IDP web server such that only TLS is supported; therefore the protocol does not need to be dynamically derived during assertion generation. This may pose other usability issues that should be discussed.

Access to non-Exostar applications, connected to the Exostar platform, requires explicit approval by the corresponding application owner prior to acceptance. Exostar, working with TSCP, may revise the assertion format provided by Exostar to an SP by including additional attributes pertinent to the R-IdP. In this model, Service Providers may make runtime decisions on whether to accept assertions, by using information on who the Identity Provider is (which may or may not be Exostar).

Required Information from Exostar

Exostar shall provide to the R-IDP the information listed in the table below.

Data element	Mandatory?	Notes
Realm name	Yes	
Federation end point	Yes	An HTTPS URL (at Exostar) to which to redirect the user's browser for token consumption

The table below lists these settings for Exostar's User Acceptance Testing (UAT) and Production environments.

Environment	Protocol and profile	Realm name	Federation end point
Production	WS-Fed/PRIP	urn:com:exostar:eag	https://eag.exostar.com/sp/prp.wsf
UAT	WS-Fed/PRIP	urn:com:exostar:eag	https://eag.exostartest.com/sp/prp.wsf