EXOSTAR

Exostar Product Specific Terms
V2.3 – December 2025

Contents

EXOSTAR PRODUCT-SPECIFIC TERMS

1. **Permitted Uses.** Depending on the Services purchased, Subscriber may use a Service to: (1) purchase products and services through the Exostar Platform,
(2) create transactions within the Exostar Platform, (3) search and select products and confirm and accept transactions, (4) determine which information, offers or inquiries to make available to which Vendors based on Subscriber's criteria.

   Subscriber may use the Services also to interact with Customers, including two-way remote use of another party's electronic and IT systems. Subscriber may not transfer, lease, loan, resell for profit, distribute or otherwise grant any rights in the Service in any form to any third party, including commercial time-sharing, rental or service bureau use.

   Subscriber may use the Services to authenticate interactions with Customers, including the facilitation of two-way remote use of another party's electronic and IT systems. Subscriber agrees that no information, other than authentication information, shall be exchanged as part of the Service.

   Subscriber may use the system to invite Supplier Users already users of the Managed Access Gateway Service to make specific Assertions using the Supplier Management Service. It is expected that Subscriber and Supplier User(s) have agreements in place between them establishing a relationship which contains terms and conditions governing their relationship and setting forth the terms and conditions on which the Assertions may be used. In the event there is no agreement between Subscriber and a Supplier User, the submission of Assertions in response to an invitation from Subscriber shall establish a relationship between the Subscriber and Supplier User. Subscriber may use the system to review completed Assertions from Supplier Users that have a relationship with the Subscriber. Subscriber shall determine and agree with Supplier User(s) which Assertions will be required by Subscriber and how such Assertions will be used. The set of Assertions collected by a given Subscriber may be different across Subscribers.

   The Service may include document transport, translation and business process compliance services. Exostar may use a third-party (a "*Servicer*"), to provide all or a portion of such services. The provision of these services may be dependent upon use of the Servicer's infrastructure, including hardware and software, and the Servicer's project management and technical resources.

2. **Limitations on Use**

   a. All use of the Service is subject to Exostar's Use Policies.
   b. **Sponsored Users**. If applicable to the Service, Sponsored Users may not utilize the Service for any use other than participating in sessions with their Sponsor. Notwithstanding the foregoing, the Subscriber shall be liable and responsible for the actions and activities of their Sponsored User(s). Subscriber is not required to have Sponsored Users and is deemed to have no Sponsored Users until such time as it has so invited a Sponsored User to participate in a session.

3. **Fees.**

   a. Fees are quoted on a per user basis for a fixed period of time. Subscriber has been given a quote for the fees Subscriber will be charged for the service, or Subscriber will receive such quote shortly, either by letter, email, or other written communication. Such quote is hereby incorporated herein by reference.
   b. In certain circumstances, Sponsored Users may arrange for the actual payment of fees due hereunder to be made on their behalf by third parties. Such payments are acceptable to Exostar provided such payments are actually made and such payments shall be considered payments made by the Sponsored User. The making of such third-party payments will in no way entitle the third party to utilize the Service hereunder. Notwithstanding the provisions of Section 3.a above, if fees have been paid, or will be paid, on a Sponsored User's behalf, the Sponsored User will not receive a quote of the fees.

4. **Definitions.** Capitalized terms used herein shall have the meanings set forth below:

   a. "*Assertions*" means self-assertions made by the Supplier User on behalf of their company or entity.

   b. *"Authorized User" or "User"* means, collectively, employees, agents or representatives of Subscriber, that Subscriber authorizes to use the Exostar Platform or any Service on Subscriber's behalf, for whom Subscriber has purchased a subscription, or for whom Subscriber has arranged for a subscription to be purchased, and the applicable fees for which subscription have been paid or are to be paid, including an individual employee or agent of Subscriber who has met the standards and is authorized to be issued a Digital Certificate. Any acts or omissions of Authorized Users and/or a User shall be deemed to be those of Subscriber for purposes of this Agreement.

   c. *"AVD" :* Microsoft Azure Virtual Desktop is Microsoft's cloud-based desktop and app virtualization service on Azure, letting users securely access personalized Windows desktops and apps from anywhere on any device,

   d. "*CMMC Ready Suite*" : CMMC Ready Suite is a bundle of Exostar cloud-based services that enable an organization seeking US DoD (aka DoW) CMMC Level 2 assessment or certification to comply with the NIST Special Publication 800-171 version 2 controls.

   e. *"Connection*" means the integrated electronic gateway through which transactions or messages are sent. Typically, this refers to an electronic link between the Subscriber and one Customer using the same data structure. Additional Customers or data structures constitute additional Connections. Different division/programs/locations of the same company may be considered as separate Connections if the data structure, data type, transport protocol, URL, business process or support requirements are unique.

   f. *"Content*" means information supplied to Customers via the Service.

   g. "*Contract Value*" means the monetary value assigned to this agreement for the term, as agreed by the Parties.

   h. *"Consent Form"* means a document, in substantially the form contained in Exhibit 4 attached hereto, evidencing an Authorized User's consent to the collection and storage of the personal identity information to be collected by the Proofing Entity

   i. *"Delegation of Authority"* means a document evidencing a chain of delegated authority from the Contract Administrator to the holder. Such document must be notarized by a public notary and in form and substance satisfactory to Exostar.

j. *'DemandLine" means the electronic document exchange service offered by Exostar allowing selling organizations to handle transactions with their customers over the Internet, including but not limited to receiving, and responding to purchase orders.*

k. *"Employment Letter"* means a letter, satisfactory in every case to Exostar and the Proofing Entity, on the official letterhead of the Subscriber signed by an authorized representative of Subscriber confirming (i) the employment of the Authorized User by the Subscriber, (ii) the full name of the Authorized User, (iii) the employee's identification number, if any, and (iv) such other information as the Subscriber typically uses to positively identify employees to third parties.

l. "*EMSD*" means Exostar Managed Secure Desktop.

m. *"ERP Company"* means a distinct business unit within an ERP, allowing for separate financial tracking, data management, and configuration.

n. "*ExoConnect"* means the electronic document exchange service offered by Exostar allowing buyers and suppliers to handle Customer transactions over the Internet, including but not limited to receiving, and responding to purchase orders.

o. *"Exostar Managed Microsoft 365"* service refers to providing the customer with a Microsoft 365 tenant that is integrated with the Exostar Platform, via an Exostar Microsoft application. This service enables its customers to 'search' and 'invite' Subscribers who are currently members of the Exostar Platform to access the new customer's Exostar Managed Microsoft 365 tenant setup. In addition, Exostar Managed Access for Microsoft 365 enables compliance with enterprise policies by providing customers with the ability to create 'Microsoft Teams workspaces' using the Exostar Microsoft Application.

p. *"Exostar Managed Microsoft 365 Add-on Services"* for the purposes of this Service Agreement means the variety of services available to supplement the Exostar Managed Microsoft 365 services, including, but not limited to, Compliant File Drop, and additional storage capacity. Add-on services maybe be purchased as part of an initial bundled service offering, or separately via a stand-alone Sales Order, Quote, or other means.

q. "*FIDO*" (Fast IDentity Online) is an open standard for strong authentication that replaces passwords with cryptographic security keys, enabling secure, phishing-resistant login through local user verification methods like biometrics, PINs, or hardware tokens. *FIDO authentication* is a secure authentication method that uses public key cryptography instead of shared secrets, allowing users to verify their identity through local actions (like biometrics, PINs, or security keys) — supporting both password-less and second-factor login options.

r. "*General Terms and Conditions*" means Addendum A to the Master Services Agreement, the document containing the general terms and conditions for use of the Exostar Platform. The General Terms and Conditions are binding on the Subscriber as part of this Platform Service Agreement and are incorporated herein by reference.

s. *"Relying Party*" means a service, site, or entity that depends on an identity provider to identify and authenticate a user who is request access to a digital resource.

t. "*Representation Materials*" means documents, records and other materials supporting the representations and warranties made by Subscriber to Exostar regarding the security protections, physical and electronic, deployed or used by Subscriber for its IT infrastructure and account, credential and security management practices.

u. "Security Validation" means the Subscriber completing and submitting the Security Questionnaire and any other Representation Materials reasonably requested by Exostar. Exostar will complete the Assessment by scoring the questionnaire, conducting follow up interviews to get the necessary context and detail, and reporting to the governing council.

v. "*Managed Access Gateway Service*" means the services offered by Exostar allowing Subscriber and Customer to interact, including, if permission is granted by the other party, remote use of the other party's electronic and IT systems. "Enterprise Access Gateway Service" means the services offered by Exostar allowing Subscriber and Customer to interact via integration of the Subscriber acting as a Remote Identity Provider asserting user authentication information to Exostar and affiliate Service Providers as described in 19. below. attached hereto. This may include Exostar service allowing Subscriber to collect certain self-assertions from their suppliers on the Exostar Platform using Industry standard forms. The Managed Access Gateway Service will be the access point to this service for Subscriber and the way Subscriber will interact with other subscribers to accept their Assertions." This service enables Subscribers to have one location that provides access to Enterprise applications for their supplier community, an ability to manage the Supplier lifecycle from onboarding to offboarding and a streamlined dashboard to view Supplier Risk Scores. The Service may also include "Form Designer" allowing Subscriber to create and update forms without the involvement of Exostar IT based on regulatory requirements thereby reducing the time to comply.

w. *"OTP Policy*" means the One Time Password policy maintained by Exostar LLC and posted on myexostar.com.

x. *"Proofing Entity"* means the entity responsible for reviewing the Consent Form, Employment Letter and other materials from an Authorized User. Exostar will inform the Subscriber of the name of the Proofing Entity by letter or electronic means not more than fourteen (14) days after the Effective Date.

y. *"Sponsor"* means a company or entity outside of Subscriber's organization also subscribing to the Service. "Sponsor" may also mean, depending on the context, an organization that supports the connection of a Relying Party or Remote Identity Provider to Exostar system.

z. *"Sponsor Managed Organization" or "SMO" or "Sponsored Organization" means an organization that is managed by a Sponsor for the purposes of accessing Sponsored Applications via the Exostar Platform. The Sponsor is responsible for onboarding, credentialing, and maintaining the SMO's access and compliance with applicable security requirements.*

aa. *"Sponsored User*" means (1) a company or entity invited by a Sponsor to participate in one or more sessions with the Sponsor, and (2) which company's, or entity's, sole use of the Service is to participate in such sessions.

bb. *"Storage Calculation True-up"* for the purposes of the Managed Microsoft 365 Service, means the storage consumed by the Subscriber in the use of the Services. Storage volume varies by license type. In the event of storage overage by Subscriber, storage shall be calculated at the end of the license term and invoiced at the price point in effect at the time of renewal.

cc. *"Supplier Management Module"*, or *"Supplier Management Module Service"*, means the service offered by Exostar allowing Subscriber to collect certain self-assertions from their suppliers on the Exostar Platform. The Managed Access Gateway Service will be the access point to this service for Subscriber and the way Subscriber will interact with other subscribers to accept their Assertions.

dd. *"SupplyLIne""* means the electronic document exchange service offered by Exostar allowing buyers and suppliers to handle Customer transactions over the Internet, including but not limited to receiving, and responding to purchase orders.

5. Exostar Employees. All those Exostar employees or contractors who have administrative access to Exostar production level systems or who have any access to any Exostar PKI or OTP systems shall be U.S. persons as defined in the International Traffic in Arms Regulations (22 CFR 120.32).

6. Managed Access Gateway Terms

For Subscribers to the Managed Access Gateway (MAG):

"*Service*" or "*Managed Access Gateway Service*", for purposes of this Service Agreement, means the services offered by Exostar allowing Subscriber and Customer to interact, including, if permission is granted by the other party, remote use of the other party's electronic and IT systems.

a. **Acceptance of the Agreement.** Subscriber, through its authorized representative hereby agrees to be legally bound by this Service Agreement, associated General Terms and Conditions, and/or the Master Services Agreement for the Exostar Platform. IF SUBSCRIBER DOES NOT AGREE TO THE TERMS OF THIS SERVICE AGREEMENT, SUBSCRIBER MAY NOT ACCESS THE SERVICE.

b. **Exostar Platform.** Subscriber is eligible for, and is automatically enrolled in, membership to the Exostar Platform at the Essential tier as part of services under this Agreement. Details of the Platform Service tiers may be found on our website:https://www.myexostar.com/knowledge-base/exostar- platform-subscription-terms-and-conditions/ To opt out customers may email customersuccess@exostar.com with their Exostar ID and the subject "Opt Out". To upgrade to another tier, customers may email customersuccess@exostar.com with their Exostar ID and the subject line "Upgrade".

7. Exostar Managed Microsoft 365 Service Terms

a. Permitted Uses.

Exostar Managed Microsoft 365 service is offered as follows:

1. Enterprise Standard Version – Exostar provisions a Managed Microsoft 365 tenant in Microsoft GCCH for an enterprise customer, such that the enterprise customer authorized user(s) can administer the usage of this product. Exostar customer users authenticate to the customer Microsoft 365 tenant and access Exostar Managed Microsoft 365 based on this Azure Gov Entra ID authentication and not Managed Access Gateway.

2. Enterprise Premium Version – Exostar provisions a Managed Microsoft 365 tenant in Microsoft GCCH for an enterprise customer, such that the enterprise customer authorized user(s) can administer the usage of this product. Exostar customer users authenticate using Exostar Managed Access Gateway to access Exostar Managed Microsoft 365 service.

3. SMB Version – Exostar provisions a customer to a Exostar Managed Microsoft 365 that supports multiple-customers (multi-tenant), such that each customer has their own collaboration workspace that is logically isolated from other customers. Access to this SMB version is based on customer users authenticating using Exostar Managed Access Gateway

1. Microsoft terms shall apply to all users and uses of this service (https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA- for-Online-Services)
2. Subscribers may use the Service only to collaborate with other authorized users and Sponsored Users on the Exostar Platform.
3. Subscriber agrees to comply with the Use Policies posted from time to time on the Exostar Platform relating to the Service.
4. License Grant. To the extent Exostar provides software to Subscriber in connection with the Service, Exostar grants Subscriber a nonexclusive, nontransferable license to use the software supplied ("Software") and end user documentation related thereto (collectively, the "Licensed Products") solely for the purpose of Subscriber's internal business use in connection with using the Service, and the Software shall be licensed only in object code form. The license granted to Subscriber does not include the right to grant sublicenses.

8. Exostar Managed Secure Desktop Service Description and Terms

1. A Cloud based service utilizing Microsoft Azure Virtual Desktop (AVD) in Azure Government cloud that enables users to access AVD using Exostar Managed Access gateway. The service provides a set of cloud-based desktop and app virtualization services including access to Exostar Managed Microsoft 365 service.

2. The cloud-based desktop services include multiple desktops, with each desktop supporting, 2 CPU's with 8 GB of memory. The desktop has Adobe PDF reader and Microsoft Edge browser installed, along with a Microsoft Windows license.

3. Microsoft terms shall apply to all users and uses of this service (https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA- for-Online-Services)
4. Subscribers may use the Service only to collaborate with other authorized users and Sponsored Users on the Exostar Platform.
5. Subscriber agrees to comply with the Use Policies posted from time to time on the Exostar Platform relating to the Service.
6. License Grant. To the extent Exostar provides software to Subscriber in connection with the Service, Exostar grants Subscriber a nonexclusive, nontransferable license to use the software supplied ("Software") and end user documentation related thereto (collectively, the "Licensed Products") solely for the purpose of Subscriber's internal business use in connection with using the Service, and the Software shall be licensed only in object code form. The license granted to Subscriber does not include the right to grant sublicenses.

9. Certification Assistant Service Description and Terms

Certification Assistant is an easy-to-use purpose-built Governance and Risk management tool to help customers manage compliance to NIST 800-171 security controls by identifying and tracking the compliance Plan of Action and Milestones.

1. TERMS OF USE

a) Subscriber and Subscriber User are required to have the Managed Access Gateway and Exostar 2 factor authentication credential to access Certification Assistant.

b) Subscriber may use the system to invite other users to participate in assessment activities, but those users must first have the Managed Access Gateway and Exostar 2 factor authentication credential to access Certification Assistant.

c) Subscriber Users may update, review and share the artifacts required for Assertions.

d) Subscriber agrees to comply with the Use Policies posted from time to time on the Exostar Exchange relating to the Certification Assistant.

10. Policy Pro Service Description and Terms

Policy Pro helps customers develop security policy documents required under CMMC.

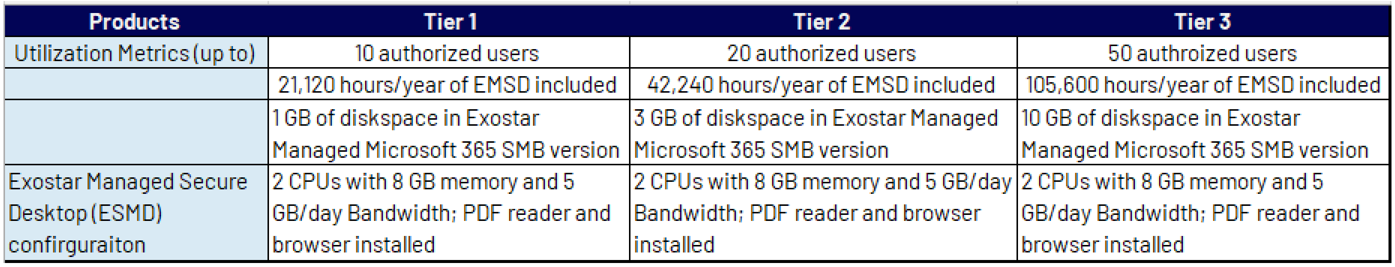
Terms of Use

a) Subscriber and Subscriber User are required to have the Managed Access Gateway and Exostar 2 factor authentication credential to access the Certification Assistant.

b) Subscriber agrees to comply with the Use Policies posted from time to time on the Exostar Exchange relating to the Certification Assistant.

11. CMMC Ready Suite Service Description and Terms

CMMC Ready suite is a bundle of the following Exostar cloud services: (a) Managed Access Gateway accessed via MFA, (b) Exostar Managed Microsoft 365 SMB version, (c) Certification Assistant, (d) Policy Pro and (e) Exostar Managed Secure Desktop. The service terms of the individual products are applicable for this Suite of services. This Suite has different tiers as outlined below:



Products	Tier 1	Tier 2	Tier 3
Utilization Metrics (up to)	10 authorized users	20 authorized users	50 authroized users
	21,120 hours/year of EMSD included	42,240 hours/year of EMSD included	105,600 hours/year of EMSD included
	1 GB of diskspace in Exostar Managed Microsoft 365 SMB version	3 GB of diskspace in Exostar Managed Microsoft 365 SMB version	10 GB of diskspace in Exostar Managed Microsoft 365 SMB version
Exostar Managed Secure Desktop (ESMD) confirguraiton	2 CPUs with 8 GB memory and 5 GB/day Bandwidth; PDF reader and browser installed	2 CPUs with 8 GB memory and 5 GB/day Bandwidth; PDF reader and browser installed	2 CPUs with 8 GB memory and 5 GB/day Bandwidth; PDF reader and browser installed

12. Additional Terms Relating to Digital Certificates

Exostar may use or accept digital certificates (each, a "Digital Certificate") in connection with authentication of users of the Service. All of Subscriber's use of Digital Certificates in connection with the Service and the Exostar Platform shall be subject to and in accordance with this Service Agreement. In particular, Subscriber agrees to the terms and conditions of the Additional Terms Relating to Digital Certificates may be found on myexostar https://www.myexostar.com/knowledge-base/policy-and-compliance/ and our Use Policy Regarding Digital Certificates (which is posted on the Exostar Platform)("Use Policy Regarding Digital Certificates"), as both may be amended by Exostar from time to time. The Use Policy Regarding Digital Certificates is incorporated into this Agreement.

13. DemandLine and SupplyLine

DemandLine Subscriber Integration Service includes:

- One ERP Company
- Unlimited customers
- Unlimited users
- One Production Environment
- One Staging Environment

SupplyLine Subscriber Integration Service includes:

- One ERP Company
- Unlimited suppliers
- Unlimited users
- One Production Environment
- One Staging Environment

a. Structural Services

1) The parties acknowledge that Subscriber user acceptance testing may not identify all items that the Subscriber or Exostar would want the software to cover ("Fallible UAT"), and that this is not a deficiency on the part of the software, the Exostar Configuration Services, Exostar, or Subscriber. The Subscriber and Exostar agree to promptly address Fallible UAT items that arise, whether requiring Services Rework (defined below) or otherwise.
2) In the event that unforeseen issues arise related to the software or Exostar configuration services (based upon Fallible UAT or otherwise), and such issues require rework and changes to the scope of or correction to the software or Exostar configuration services ("Services Rework"), then: (i) to the extent such Services Rework is the result of Subscriber's failure to perform its obligations under this Agreement or based upon Subscriber's or its employee's acts then Subscriber shall solely bear such costs; (ii) to the extent such Services Rework is the result of Exostar's failure to perform its obligations under this Agreement or based upon Exostar's acts then Exostar shall solely bear any increased costs (including all labor costs) associated with such Services Rework, up to the limitation of liability in the general terms and conditions incorporated in this Agreement.
3) Subject to Subscriber's use of the services' functionality via services' APIs, Subscriber authorizes Exostar to act as Subscriber's agent to communicate with Subscriber's customers on Subscriber's behalf for the services provided by the services. Exostar shall send information to or receive information from Subscriber's customers, provided that (a) Subscriber is responsible for the accuracy and validity of all information provided to Exostar, (b) Subscriber's failure to provide accurate and valid information may result in actions taken against Subscriber's customer; and (c) Exostar is not responsible for incorrect or invalid information provided by Subscriber or Subscriber's customers through the services. Subscriber represents and warrants that it has the authority, granted by its customers, to retrieve confidential information from its customers' secure systems and that Exostar, acting on Subscriber's behalf, has the authority to retrieve such confidential information and access such secure systems of Subscriber's customers.

14. Supply Chain Platform for Information and Process Management Service Terms

Customer Requests

Exostar agrees to promptly notify Subscriber if Subscriber's Customer notifies Exostar that it wants to buy goods or services from Subscriber via the Exostar Platform. In Exostar's notification to Subscriber, Exostar will specify, to the extent Exostar is able to determine: (1) the name of the Customer submitting the request, and (2) the information (or the Content), if any, requested by the Customer and Customer's instructions to the Subscriber for transmission of the requested information (or Content). Solely for purpose of this Service Agreement, the term "information" as used in this Section 4 is intended to refer to purchase orders and similar materials.

After Subscriber receives Exostar's notification, Subscriber must notify Exostar in writing whether Subscriber accepts or rejects the Customer's request in the manner set forth below:

To accept the Customer's request, Subscriber must notify Exostar of Subscriber's acceptance and deliver any requested information (or Content), if any.

To reject the Customer's request, Subscriber must notify Exostar of Subscriber's rejection.
If Subscriber does not accept or reject(as provided herein) within the time period previously agreed upon by Subscriber and Subscriber's Customer, Subscriber will be deemed to have rejected or accepted the request as per the agreement between Subscriber and Subscriber's Customer; *provided, however*, if Subscriber and Subscriber's Customer have no time period within which a request must be accepted or rejected or no agreement as to acceptance or rejection of Customer requests, then the request will be neither accepted nor rejected.

If Subscriber accepts the Customer's request and Content is required, Subscriber agrees to promptly deliver the required Content to Exostar in an electronic format that includes the product part number and extension, unit of measure, an abbreviated description of the product, price of the product, currency code and additional recommended or necessary data fields. If the Content is not provided as specified, Exostar may return it to Subscriber for correction. Subscriber understands that certain Content may require Subscriber to enter into a Publisher Service Agreement with Exostar to deliver the requested Content and failure to do so may prevent the required Content from being delivered. Notwithstanding the foregoing, both Parties also understand that execution of this Agreement is not intended to obligate Subscriber to enter into a Publisher Service Agreement.

Fees. Current pricing and tier descriptions are available on the Supply Chain Platform Membership page https://www.myexostar.com/?ht_kb=supply-chain-platform-scp-supplier-membership

15. Federated Identity Service Terms

"Federated Identity Service", for purposes of this Service Agreement, means the set of security services that provide assurance about the identity of a party and its related attributes to a relying party. The set of services also include ancillary services that enable trust among users that exchange identity attributes using the identity federation mechanism, as well as discovery services that enable discovery of identity certificates used for encryption.

a. Service Description

Introduction

Exostar provides security management services as part of its Federated Identity Service. These services are compliant to policy and may include the following, as appropriate:

i. Key generation/storage
ii. Certificate generation, update, re-key, and distribution
iii. Certificate revocation list generation and distribution
iv. Repository management of Certificate related items
v. System management functions (e.g. security audit, configuration management, archive)
vi. Identity proofing and authentication for Authorized Users

Service Scope

The Service may issue up to three (3) Digital Certificates to support:

- Authentication
- Digital signature
- Encryption

Certificates are valid for up to 3 years. Under the Federated Identity Service, Exostar is responsible for operating the core Public Key Infrastructure ("PKI") and for verifying the identity of Authorized Users. Subscriber authorizes Exostar to issue Certificates on its behalf. The following „name spaces‟ are controlled by Exostar, unless otherwise agreed upon in this Service Agreement: FIS.EVINCIBLE.COM

Unique Roles and Responsibilities

a. Exostar

i. Exostar maintains responsibility for operating the core PKI and for verifying the identity of Authorized Users.

ii. Exostar ensures that all aspects of the Certificate Authority service, operations, and infrastructure related to Certificates are compliant under the Certificate Policy

iii. Exostar ensures that all aspects of the Registration Process related to Certificate issuance are compliant under the Policy

b. External Auditors

The External Auditors are independent from Exostar, engaged by Exostar as required by the Certificate Policy to perform an independent review and validation of Federated Identity Service to ensure that the Federated Identity Service is in compliance with the Certificate Policy.

c. Identity Proofer

These individuals, working for or on behalf of Exostar, are responsible for performing identification and initial authentication functions as defined in the Certificate Policy. Exostar will instruct these individuals on the procedures to be used to perform these activities.

d. Subscriber

Subscriber agrees that Exostar will escrow the encryption private keys issued to Authorized Users.

i. Subscriber agrees to appoint one or more individuals to act on its behalf in the following roles:

a. Federated Identity Service Administrator ("FIS Administrator")
This individual, working for Subscriber, has overall responsibility for approval of issuance of Certificates. This person has the authority to approve issuance of Certificates within their organization, and responsibility for initiation of revocation of those Certificates when the Authorized User is no longer affiliated with the organization.

b. Organization Administrator ("Organization Administrator")
This individual, working for the subscriber, has responsibility for confirming the association between the Authorized User and the Subscriber. The Organization Administrator may also indicate that an Authorized User is no longer affiliated with the Subscriber.

e. Authorized User

In addition to the responsibilities set forth in the General Terms and Conditions, Authorized Users have the following obligations under this Service Agreement:

- Accurately represent themselves in all communications with Exostar and the Identity Proofer.
- Present certain personal identifying information to the Identity Proofer, as instructed.
- Protect their private keys at all times.
- Notify, in a timely manner, the Federated Identity Service if they suspect their private keys have been compromised or lost.
- Abide by all other terms, conditions, and restrictions as applicable.
- Attest to these obligations by signing the Authorized User Agreement (Exhibit 2 attached hereto), presented during the in person proofing activity.

f. Management Overview of a Registration Process. The enrollment process for the Federated Identity Service includes the following steps (unless instructed otherwise by an authorized person from Exostar):

- A prospective Authorized User completes an online enrollment form.
- The Subscriber approves the Authorized User's request
- Scheduling of in-person proofing
- The prospective Authorized User appears before the Identity Proofer for in-person proofing
- Exostar Trusted Agents provide final verification that the process was successfully completed and in accordance with Policy.
- The Authorized User receives an approval email with instructions for obtaining their certificates

g. Fees

i. Subscriber agrees to pay Exostar for the Services in the manner set forth in this Service Agreement. In certain circumstances Subscribers may arrange for the actual payment of fees due hereunder to be made on their behalf by third parties on a yearly basis. Such payments are acceptable to Exostar provided such payments are actually made and such payments shall be considered payments made by the Subscriber. The making of such third party payments will in no way entitle the third party to utilize the Service.

ii. Subscriber must pay the Federated Identity Subscription Fee at the time of registration or Exostar will invoice Subscriber at the time of enrollment or renewal for the Service, but no Service will be provided until payment is received. Failure to receive Subscription fees upon registration or renewal will result in termination of the Subscribers service.

iii. Subscriber agree to calculate and pay all taxes, duties or charges of any kind (including withholding or value added taxes) that may be imposed by any federal, state, local, national, provincial or other governmental entity for Subscriber's use of the Services, excluding only those taxes based solely on our property or net income. Subscriber agrees to hold Exostar harmless and indemnify Exostar from all claims and liabilities that arise from Subscriber's failure to report or pay any such taxes, including duties, tariffs or charges.

iv. Subscriber agrees that Subscriber will not, for any reason, subtract or offset any amounts Exostar may owe Subscriber from any fees or charges that Subscriber owes Exostar.

h. Term. The initial term of this Service Agreement is defined at the time of registration and will be either for a period of twelve (12) months or for a period of thirty-six (36) months commencing on the Effective Date.

i. Termination. In addition to other termination rights in the Master Services Agreement for the Exostar Platform, either Party may terminate the Service upon thirty (30) day prior written notice to the other Party.

16. Supplier Management Module

Special Provisions applicable only to Supplier Management Module Service:

Indemnity. Without limiting any other indemnification obligation Subscriber may have, Subscriber agrees to indemnify, defend, and hold Exostar, the application vendor(s) and their licensors (including affiliates, officers, directors, employees, and agents) harmless from and against any loss, injury, demand, cost, expense, or claim of any kind or character, including but not limited to attorneys' fees, arising out of or related to any use or misuse of the Supplier Management Module by Subscriber or Subscriber's Supplier Users.

Equitable Remedies. Subscriber agrees that because of the unique nature of the Supplier Management Module, and the proprietary rights of Exostar therein, breach of this Service Agreement by Subscriber would irreparably harm Exostar, and monetary damages would be inadequate compensation. Subscriber further agrees that Exostar shall be entitled to preliminary and permanent injunctive relief to enforce the provisions of the Master Services Agreement for the Exostar Platform.

17. Enterprise Access Gateway Terms

b. Security Validation.

i. In connection with the Services provided by Exostar hereunder, Subscriber agrees that Subscriber shall:

1. When requested by Exostar, but in no event more often than annually (except in connection with dispute resolution or when required by authorities or otherwise necessary to the provision of Services in which case as often as needed), make available to Exostar (or its agents, at the request of Exostar) for examination, reproduction and inspection during validation assessments or otherwise, all Representation Materials necessary to validate that the security protections, physical and electronic, deployed and used by Subscriber are consistent with the representations and warranties made by Subscriber under this Service Agreement; and

2. From the Effective Date and for a period of no less than three (3) years after the termination of this Service Agreement, retain the Representation Materials; and

3. Allow Exostar and its agents full and reasonable access to Subscriber's premises and the Representation Materials to conduct validation assessments; and

4. Complete and submit to Exostar annual updated and Representation Materials. The initial term R-IDP Security Questionnaire is attached to this Service Agreement as Exhibit 3 and incorporated herein by reference.

c. A Security validation will be conducted by Exostar. Exostar will nominate the Subscriber to the appropriate governing council(s). Approval by the Sponsor and/or Relying Party(s) and a passing or conditional passing score on the R-IDP Security Questionnaire is a condition precedent to access to Exostar's production environment. Scoring requirements are provided in Exhibit 3.

d. Subscriber shall submit a new Security Questionnaire that achieves a passing score or attest to the answers on an existing questionnaire with a passing score annually as a condition precedent to a renewal term of the Service Agreement. By renewing the Service Agreement subscriber attests that the controls are the same or better than that of the initial term Security Validation.

e. Subscriber agrees to undergo an additional Security Validation when additional Relying Party(s) is added to Subscriber's Service.

f. A Security Validation shall be conducted (i) upon reasonable notice, (ii) during normal business hours, (iii) in a manner that does not unduly interfere with Subscriber's business, and (iv) at the location(s) where Subscriber's Representation Materials and infrastructure are normally maintained, unless the Parties agree in writing to another location.

g. Subscriber shall notify Exostar within 24 hours of any breach of Subscriber's information systems. Notifications shall be provided to the Subscriber's main point of contact at Exostar and emailed to: CIRT@exostar.com. Subscriber shall also notify any Sponsor and Relying Party of EAG service within 24 hours.

h. Any material breach of Subscriber's information systems shall be considered a default for which Exostar, in its sole discretion, may immediately suspend or revoke access and the Service.

i. Termination of Services.

i. Exostar reserves that right to terminate this Service with immediate effect unless the completed R-IDP Security Questionnaire, below, is received prior to the start of each succeeding twelve (12) month period. If the Services are terminated for any reason, Exostar has the right to immediately discontinue Subscriber's access to the Services and to remove Subscriber's authentication information, if any, from the Exostar Platform. Exostar has the right to immediately discontinue Subscriber's access to the Exostar Platform if Subscriber has not subscribed to any other service on the Exostar Platform.

ii. Subscriber agrees to promptly discontinue using the Services, and to discontinue using any Confidential Information that Exostar has given to Subscriber relating to the Services. Notwithstanding the foregoing, (1) Subscriber will be responsible for payment of fees for Services received prior to any termination, and (2) under no circumstances will refunds will be provided by Exostar as a result of any termination hereunder.

j. Additional Representations and Warranties

i. Exostar warrants to Subscriber that Exostar shall not intentionally install or trigger a lockup program or device that in any manner interferes with Subscriber's authorized use of the Software.

ii. Exostar warrants that, to Exostar's knowledge, the Software as delivered to Subscriber does not contain any computer code: (a) designed to disrupt, disable, harm or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of the Software, or any other associated software, firmware, hardware, computer system or network (sometimes referred to as "viruses" or "worms"); (b) that would disable the Software or impair in any way its operation based on the elapsing of a period of time, advancement of a particular date or other numeral (sometimes referred to as "time bombs," "time locks," or "drop dead" devices); or (c) that would permit Exostar or any third party to access the Software to intentionally cause such disablement or impairment (sometimes referred to as "lockups," "traps," "access codes," or "trap door" devices), or any other similar harmful, malicious or hidden procedures, routines or mechanisms which would cause the Software to cease functioning or to damage or corrupt data, storage media, programs, equipment or communications, or otherwise interfere with operations. Exostar agrees that, in the event any such computer code is found to have been introduced into the Software as delivered to Subscriber, Exostar shall use commercially reasonable efforts to assist Subscriber in removing such code and in mitigating and restoring the effects of any loss of operational efficiency.

iii. Subscriber represents that for the term of this Agreement it will be a holder of Microsoft SharePoint Client Access Licenses (CALs) for its enterprise users.

18. Use of UAT and DEV Environments

a. Availability of the UAT and DEV environments shall be provided on a commercial best-efforts basis. No service levels or guarantees (including uptime, performance, response or resolution times, recovery time objections, or error-free operation) apply to the UAT or DEV environments, except as expressly outlined below.
b. Exostar may, without liability, suspend, limit or modify access to the UAT and Dev environments for maintenance, upgrades, security remediation, environment refreshes, or other operational reasons, including unplanned outages. Where practicable, Exostar will use reasonable efforts to provide prior notice of scheduled maintenance.
c. Service credits, remedies, or penalties applicable to production services do not apply to the UAT or Dev environments. Subscriber acknowledges that intermittent unavailability, performance degradation, data loss in non-production environments (including environment resets), and feature differences may occur.
d. Subscriber is responsible for ensuring that no live production data (including personal data, regulated data, or confidential information) is loaded into the UAT or Dev environments unless expressly permitted in writing by Exostar. Exostar shall have no obligation to back up or retain data in the UAT or Dev environments.
e. Subscriber shall not rely on the UAT or Dev environments for business continuity or disaster recovery. Exostar disclaims, to the maximum extent permitted by law, all warranties, express or implied, with respect to the UAT and Dev environments, and shall have no liability for unavailability, loss of data, delays, or failures related to these environments.

19. EAG Service Agreement Service Description

This section describes Exostar's Enterprise Access Gateway Service as it pertains to the integration of the Subscriber acting as an 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:

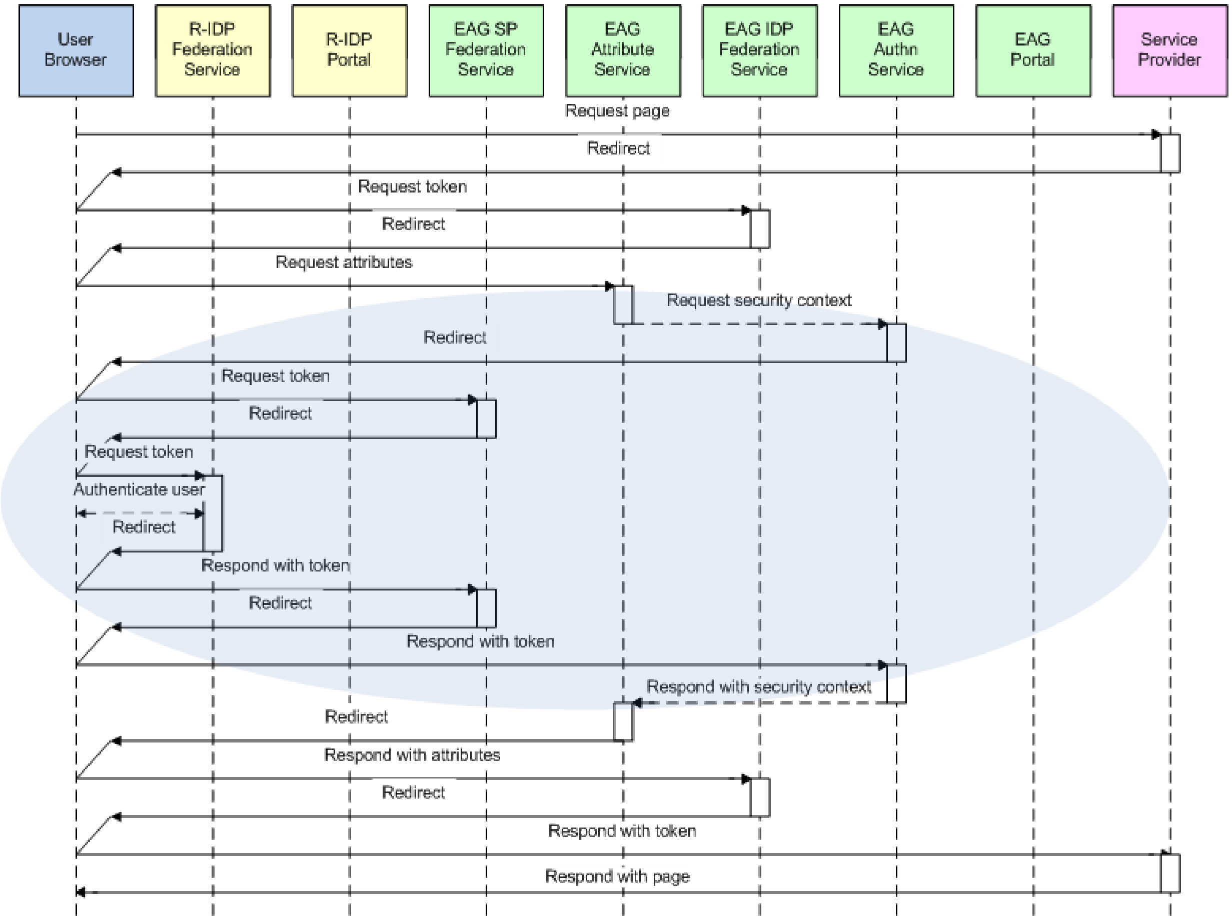


Figure 1 – EAG Authentication Flows

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: EAG Service Agreement 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 (v1.0)

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: bae-greenlink Example: us-dod	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 for starting list for this set of authenticators	password	Application account user-id and password	Mandatory	
			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)		
			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 assigned to the user.	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		
Std	proofinglevel		level_1	No Vetting Process	Mandatory	

		User identity proofing level	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		

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 certificates.

Exhibit 3: R-IDP Security Questionnaire

Instructions & Notes

Instructions:

- Please answer all the questions in rows 8 through 12 below.
- Please answer the questions on the remaining tabs in this questionnaire. Complete answers are comprised of a Yes/No response and specific details of compliance.
- Please complete and submit this security questionnaire to Exostar within 5 business days of receipt.
- Exostar will set a conference call with you to review the results of the security questionnaire. Please ensure to include appropriate members that can elaborate on all controls outlined in the security questionnaire.

Note:

- The highlighted controls in yellow have been identified as "core controls". Each RIDP must be compliant with all core controls to receive a passing score.
- The Security Questionnaire is scored on a three-tiered basis: Pass, Conditional Pass, Not Pass.
  - Pass (Green): The RIDP is compliant with all core controls and at least 80% of all security controls
  - Conditional Pass (Yellow): The RIDP is compliant with all core controls but less than 80% of all security controls. The EIDP must commit to be compliant with all core controls and 80% of all security controls at least 30 days before their annual renewal.
  - Not Passing score (Red): The RIDP is not compliant with all of the core controls and not compliant with at least 80% of all security controls

General Questions

Questions	Answers
Company Name:	
Questionnaire Completion Date:	
Name and title of those who answered the questionnaire	

Number of employees in the company:	
Number of People in the IT Security Organization:	
Number of people on the Identity & Access Management team:	
Exostar Assessment Team Members:	
Assessment Date:	
AssessmentRecommendation: (Security Posture Sufficient or Insufficient)	
ESEC Decision:	
ESEC Decision Date:	

Security Certifications		
Control	Are you compliant? (Yes / No)	How are you compliant?
Please Identify any certifications which your company has obtained any of these certifications: SSAE 16: SOC 2 Type 2, ISO27001, CertiPath, SAFE, and FICAM		

Does your company use PKI based authentication?		

Security Policy		
Control	**Are you compliant? (Yes / No)**	**How are you compliant?**
Does your organization have a security Policy?		
Is your security policy based on an industry framework (e.g. ISO 27002, etc.)?		
What is the business role of the individual who approves the policy and revisions (e.g. CSO, Directory of Information Security, etc.)		
How often is the policy revised?		
Are the results of the review documented and reviewed by management?		

External Parties		
Control	**Are you compliant? (Yes / No)**	**How are you compliant?**

Does you company have an industry standard information security management framework implemented? (ex. ISO27001, NIST RMF, NIST 800-53, etc)		

Identify external security groups with whom your company maintains a relationship: - Security vulnerability monitoring lists (SANS, etc) - Security focused products/service vendors		
What is the title of the individual(s) with overall responsibility for implementation and maintenance of security?		
Are security responsibilities identified in the job descriptions of individuals with security implementation duties?		
Has every external party who has contracted with your company executed a confidentiality agreement which defines requirements for information protection?		
Who is responsible for ensuring that confidentiality agreements are maintained for all companies with whom your organization maintains a relationship that involves exchange of sensitive information?		
Who is responsible for defining the terms of the confidentiality agreements developed by your organization and signed by business partners?		
How often are the terms of the confidentiality agreements reviewed to determine if they should be updated?		

Are third parties involved in the operation of any identity management infrastructure; and if so, have they entered into an agreement with your organization which identifies the required policies and controls that they must observe in operating identity infrastructure on behalf of your organization?		

Human Resources Security		
Control	**Are you compliant? (Yes / No)**	**How are you compliant?**
Do job descriptions for employees identify security as a job function?		
Are securityresponsibilitiesincluded in employment contracts or other agreements?		
Are contractors and third parties responsible for maintaining similar arrangements when dealing with company information?		
Are employees provided with regular security awareness training ?		
Are procedures in place governing exit from or transfer within the organization?		
Are third parties required to implementequivalent procedures for exiting or transferring employees?		

Physical & Environmental Security

Control	Are you compliant? (Yes / No)	How are you compliant?
Are corporate facilities protected from unauthorized access?		
Is identificationrequired to gain access to corporate and hosting facilities?		
Is the date and time of entry recorded for all access to facilities?		
Are visitors required to wear special badges or are escorted when at the facility?		

Communications & Operations

Control	Are you compliant? (Yes / No)	How are you compliant?
Has your company published internal SOPs and incident response procedures for management of Identity infrastructure?		
Has your company implemented change control procedures governing modification of Identity infrastructure or data?		
Does your company leverage role segragation in the management of Identity infrastructure?		

Does your company implement countermeasures against malware and other malicious code? Examples can include anti-virus software, filtering web proxies, or other mechanisms.		
Does your company segregate systems hosting sensitive data using network segmentation?		
Is sensitive informationencrypted in transit over public networks? (Ex. Any sensitive information, Individual Info such as logins by users to access corporate resources or Aggregate information such as site to site identity repository replication)		
Is sensitive information encrypted at rest?		
Has your company developed information exchange policies governing transmission of company sensitive identity information outside of the company?		
Are users trained on the proper handling of personal or company sensitive information which may be used in Social Engineering attacks?		
Does your company activate security audit logging on Identity management infrastructure components?		
Are audit logs centrally maintained and archived to support investigation? (Ex. SIEM)		
Are audit logs centrally monitored to detect and identify security issues?		

Are audit logs protected from unauthorized tampering?		
Are system administrator activities logged and audited?		

Access Control		
Control	**Are you compliant? (Yes / No)**	**How are you compliant?**
Does your company have policies governing access control to sensitive identity information?		
Do your policies dictate explicit authorization for access to sensitive identity information for authorized business roles?		
Does your company have policies governing the allocation of access rights to corporate resources?		
Do corporate access provisioning policies govern: ● Initial registration? ● Role changes which require different access privileges? ● De-registration of users who sever their relationship with your company?		
Does your company access management policy include a periodic review of access rights?		
Are assignment of administrative privileges to identity management infrastructure componentsaudited and regularly reviewed?		

Are users issued unique identifiers, such that the actions on systems can be traced to a single individual?		
Does user security training include requirements for managing passwords or other credentials, such as OTP tokens?		
Are users required to acknowledge receipt of training and agree to abide by requirements?		
Does your company implement additional controls to control access to services that are available over the internet?		
Does your company required Multi- Factor Authentication (MFA) for all remote access?		
Is access to corporate resources restricted for those accessing resources from the internet?		
For systems which require user managed passwords, what password quality enforcement mechanisms have been implemented?		

For systems which require user managed passwords, does your company require the use of complex passwords (minimum of 8 characters, passwords that contain: upper and lower case letters, numbers, and symbols)		
Does your company require password reuse settings of at least 12? (ex. you can't use the last 12 passwords again)		
Does your company require password failed attempt lockout of 5 attempts?		
Do user workstations, and servers supporting the identity management infrastructure implement least privilege mechanisms like Microsoft's User Account Control (UAC) system?		
Does your company have policies governing the use of company and personal mobile devices (iPhones, etc.) to access company resources and data?		
Does your company use for Mobile Device Management (MDM)?		
Does your MDM require, at least a 8 character passcode, data wipe after 10 failed login attempts, and data encryption on the mobile device?		
Does your company publishpolicies on teleworking which address the security of teleworking sites?		

Do policies governing teleworking sites include the following: ● limitations on storage of sensitive data at remote sites. ● limitations on the use of personally owned computing equipment to access sensitive data at remote sites. ● guidelines for configuration of home networks (especially wireless networks) to ensure that sensitive corporate data is protected in transit ● revocation of access rights and return of equipment when remote users leave the company		

Information Security Incident Management		
Control	**Are you compliant? (Yes / No)**	**How are you compliant?**
Does your company have an incident response team?		
Has your company developed event reporting andescalation procedures for security incidents?		
Do company security policies require all employees and contractors to report suspicious events related to company systems or data?		

Are company administrators required by policy to report any potential security weaknesses observed in managed systems?		

Compliance		
Control	**Are you compliant?(Yes / No)**	**How are you compliant?**
Does your company's training include information about relevant laws and regulatory requirements?		
Have your company'spolicies and procedures been reviewed and approved by legal counsel?		
Are security policies and procedures regularly reviewed to ensure ongoing compliance with existing or new regulations and laws?		

Exhibit 4

FORM OF CONSENT

(This form or a substantially similar form is to be signed by the Authorized User during in-person proofing)

For Storage of Personal Identifiable Information

The undersigned hereby consents to the collection and storage in the United States (by Exostar LLC and/or their authorized representatives or agents) of such personal identifying information concerning the undersigned as may be determined necessary by Exostar, including, but not limited to, the following:

Full name
Signature (in electronic and manual forms) Birth date
Identification card with photo (e.g., a driver's license, an ID card issued by a federal, state, or local government entity, such as a Passport number and issuing country)
Evidence of citizenship and/or immigration status

The undersigned agrees that such information may be stored for a minimum of ten (10) years and six (6) months following its collection. Such information may be stored and utilized for purposes of the delivery of Federated Identity Service (as defined in the Service Agreement) offered by Exostar.

Printed Name of Applicant:

Signature of Applicant: Date of

Consent: