



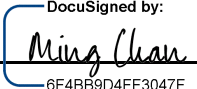
Exostar One-Time Password (OTP) Policy

Version 2.4

February 14, 2023

Exostar One-Time Password (OTP) Policy v2.

Signature Page

X  6F4BB9D4FF3047F...

Exostar PMA Chair

Ming Chan

Manager, Governance & Engineering

2/16/2023

Table of Contents

1	INTRODUCTION	7
1.1	Overview	8
1.1.1	One-Time Password Policy (OP)	8
1.1.2	Relationship between this Policy and the OTP Practices Statement (OPS)	8
1.1.3	Scope	8
1.2	Federation Participants	8
1.2.1	Authorities	8
1.2.2	Exostar Identity Management Services	10
1.2.3	Participants	11
1.2.4	Relying Parties	11
1.2.5	Applicability	11
1.3	Token Usage	11
1.3.1	Appropriate Token Uses	11
1.3.2	Prohibited Token Uses	11
1.4	Policy Administration	11
1.4.1	Organization administering the document	11
1.4.2	Contact Person	12
1.4.3	Person Determining OP and OPS Suitability	12
1.4.4	OP and OPS Approval Procedures	12
1.4.5	Waivers	12
2	PUBLICATION & REPOSITORY RESPONSIBILITIES	13
2.1	Public Repositories	13
2.2	Authoritative Private Repositories	13
2.3	Repository Obligations	13
2.4	Access Controls on Repositories	13
3	IDENTIFICATION & AUTHENTICATION	14
3.1	Naming	15
3.1.1	Types of Names	15
3.1.2	Need for Names to be Meaningful	15
3.1.3	Recognition, Authentication & Role of Trademarks	15
3.1.4	Name Claim Dispute Resolution Procedure	15
3.2	Initial Identity Validation	15
3.2.1	Method to Establish Exostar MAG Account	15
3.2.2	Authentication of Organization Identity	15
3.2.3	Authentication of Individual Identity	15
3.2.4	Identification and Authentication for OTP Re-Sync Requests	16

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

3.2.5	Authentication for Level 3 Proofing	16
3.2.6	Identification and Authentication for Credential Reactivation after Revocation	17
3.3	Identification and Authentication for Revocation Request	17
3.4	Identification and Authentication for Credential Replacement	17
3.5	Subscriber Assertion of US Person Status	18
4	CREDENTIAL LIFE-CYCLE OPERATIONAL REQUIREMENTS	19
4.1	Subscriber Organization Application	19
4.1.1	Submission of Credential Application to Exostar	19
4.1.2	Enrollment Process and Responsibilities	19
4.2	Hardware Token Production and Shipment	19
4.2.1	Hardware Token Production and Key Handling	19
4.2.2	Hardware Token Shipment	20
4.2.3	Hardware Token Seed File Delivery to Exostar	20
4.2.4	Hardware Token Seed File Management	20
4.3	Subscriber Credential Application	20
4.3.1	Submission of Credential Application to Exostar	20
4.3.2	Enrollment Process and Responsibilities	20
4.4	Level 2 Credential Application Processing	20
4.4.1	Performing Identification and Authentication Functions	20
4.4.2	Approval or Rejection of Credential Applications	20
4.4.3	Time to Process Credential Applications	21
4.5	Credential Issuance	21
4.6	Credential Activation	21
4.6.1	Conduct Constituting Credential Acceptance	21
4.7	Hardware Token Replacement	21
4.7.1	Circumstance for Token Replacement	21
4.7.2	Who may Request Replacement	22
4.7.3	Processing Token Replacement Requests	22
4.7.4	Notification of New Token Issuance to Subscriber	22
4.7.5	Conduct Constituting Acceptance of a Renewal Token	22
4.8	Hardware Token Re-Sync	22
4.8.1	Circumstance for Token Re-Sync	22
4.8.2	Who may Request Token Re-Sync	22
4.8.3	Processing Token Re-Sync Requests	22
4.8.4	Notification of Token Re-Sync to Subscriber	22
4.9	Credential Revocation and Suspension	22
4.9.1	Circumstance for Revocation of a Credential	22
4.9.2	Who Can Request Revocation of a Credential	23

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

4.9.3	Procedure for Revocation Request	23
4.9.4	Revocation Request Grace Period	23
4.9.5	Time within which Exostar must Process the Revocation Request	23
4.9.6	Circumstances for Credential Suspension	23
4.9.7	Who can Request Credential Suspension	23
4.9.8	Procedure for Credential Suspension Request	23
4.9.9	Limits on Credential Suspension Period	23
4.10	Level 3 Remote Proofing Service	24
4.10.1	Application	24
4.10.2	Processing	24
4.11	Level 3 Binding via Postal Delivery	26
4.11.1	Application	26
4.11.2	Processing	26
4.12	Level 3 Video Proofing	27
4.12.1	Application	27
4.12.2	Processing	27
4.13	Level 2 and 3 Authentication to MAG, SAM, BAID, and ProviderPass	29
4.13.1	OTPS Authentication	29
4.13.2	SMS Authentication	29
4.13.3	IVR Authentication	29
4.13.1	APP Authentication	30
4.14	End of Subscription	30
5	FACILITY MANAGEMENT & OPERATIONAL CONTROLS	32
5.1	Physical Controls	32
5.1.1	Site Location & Construction	32
5.1.2	Physical Access	32
5.1.3	Power and Air Conditioning	33
5.1.4	Water Exposures	33
5.1.5	Fire Prevention & Protection	33
5.1.6	Media Storage	33
5.1.7	Waste Disposal	33
5.1.8	Off-Site backup	34
5.1.9	Third Party Facility Controls (RPS, SMS, IVR, and APP Providers)	34
5.2	Procedural Controls	34
5.2.1	Trusted Roles	34
5.2.2	Number of Persons Required per Task	35
5.2.3	Identification and Authentication for Each Role	36

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

5.2.4	Roles Requiring Separation of Duties	36
5.3	Personnel Controls	36
5.3.1	Qualifications, Experience, and Clearance Requirements	36
5.3.2	Background Check Procedures	37
5.3.3	Training Requirements	37
5.3.4	Retraining Frequency and Requirements	37
5.3.5	Job Rotation Frequency and Sequence	37
5.3.6	Sanctions for Unauthorized Actions	37
5.3.7	Independent Contractor Requirements	37
5.3.8	Documentation Supplied To Personnel	37
5.4	Audit Logging Procedures	38
5.4.1	Types of Events Recorded	38
5.4.2	Frequency of Processing Audit Logs	41
5.4.3	Retention Period for Audit Logs	41
5.4.4	Protection of Audit Logs	41
5.4.5	Audit Log Backup Procedures	42
5.4.6	Audit Collection System (internal vs. external)	42
5.4.7	Notification to Event-Causing Subject	42
5.4.8	Vulnerability Assessments	42
5.5	Records Archival	Error! Bookmark not defined.
5.5.1	Types of Records Archived	42
5.5.2	Retention Period for Archive	43
5.5.3	Protection of Archive	43
5.5.4	Archive Backup Procedures	43
5.5.5	Requirements for Time-Stamping of Records	43
5.5.6	Archive Collection System (internal or external)	43
5.5.7	Procedures to Obtain & Verify Archive Information	43
5.6	Key Changeover	44
5.7	Compromise and Disaster Recovery	44
5.7.1	Incident and Compromise Handling Procedures	44
5.7.2	Computing Resources, Software, and/or Data are Corrupted	44
5.7.3	Private Key and OTPS Compromise Procedures	45
5.7.4	Business Continuity Capabilities after a Disaster	45
5.8	OTPS Termination	45
5.8.1	Subscriber Termination	45
5.8.2	Organization Termination	45

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

5.8.3	Service Termination	46
6	TECHNICAL SECURITY CONTROLS	47
6.1	Key Pair Generation and Installation	47
6.1.1	Key Pair Generation	47
6.1.2	Private Key Delivery to Subscriber	47
6.1.3	Public Key Delivery to Token Issuer	47
6.1.4	OTPS and Transport Key Delivery to Relying Parties	47
6.1.5	Key Sizes	47
6.2	Private Key Protection and Cryptographic Module Engineering Controls	48
6.2.1	Cryptographic Module Standards and Controls	48
6.2.2	Private Key Multi-Person Control	48
6.2.3	Private Key Escrow	48
6.2.4	Private Key Backup	48
6.2.5	Private Key Archival	48
6.2.6	Private Key Transfer into or from a Cryptographic Module	48
6.2.7	Private Key Storage on Cryptographic Module	48
6.2.8	Method of Activating HSM-Controlled Keys	48
6.2.9	Methods of Deactivating HSM-Controlled Keys	49
6.2.10	Method of Destroying HSM-Controlled Keys	49
6.2.11	Cryptographic Module Rating	49
6.3	Activation Data	49
6.3.1	Activation Data Generation and Installation	49
6.3.2	Activation Data Protection	49
6.3.3	Other Aspects of Activation Data	49
6.4	Computer Security Controls	49
6.4.1	Specific Computer Security Technical Requirements	49
6.4.2	Computer Security Rating	50
6.5	Life-Cycle Technical Controls	50
6.5.1	System Development Controls	50
6.5.2	Security Management Controls	51
6.5.3	Life Cycle Security Controls	52
6.6	Network Security Controls	52
6.7	Time Synchronization and Time Stamping	53
6.8	High Availability Architecture	53
7	[RESERVED]	53
8	COMPLIANCE ASSESSMENTS	54
8.1	Frequency or Circumstances of Assessments	54

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

8.2	Identity and Qualifications of Assessor	54
8.3	Assessor’s Relationship to Assessed Entity	54
8.4	Topics Covered by Assessment	54
8.5	Actions Taken as a Result of Deficiency	54
8.6	Communication of Results	55
9	OTHER BUSINESS AND LEGAL MATTERS	55
9.1	Use and Governing Agreements	55
10	ACRONYMS & ABBREVIATIONS	56

1 INTRODUCTION

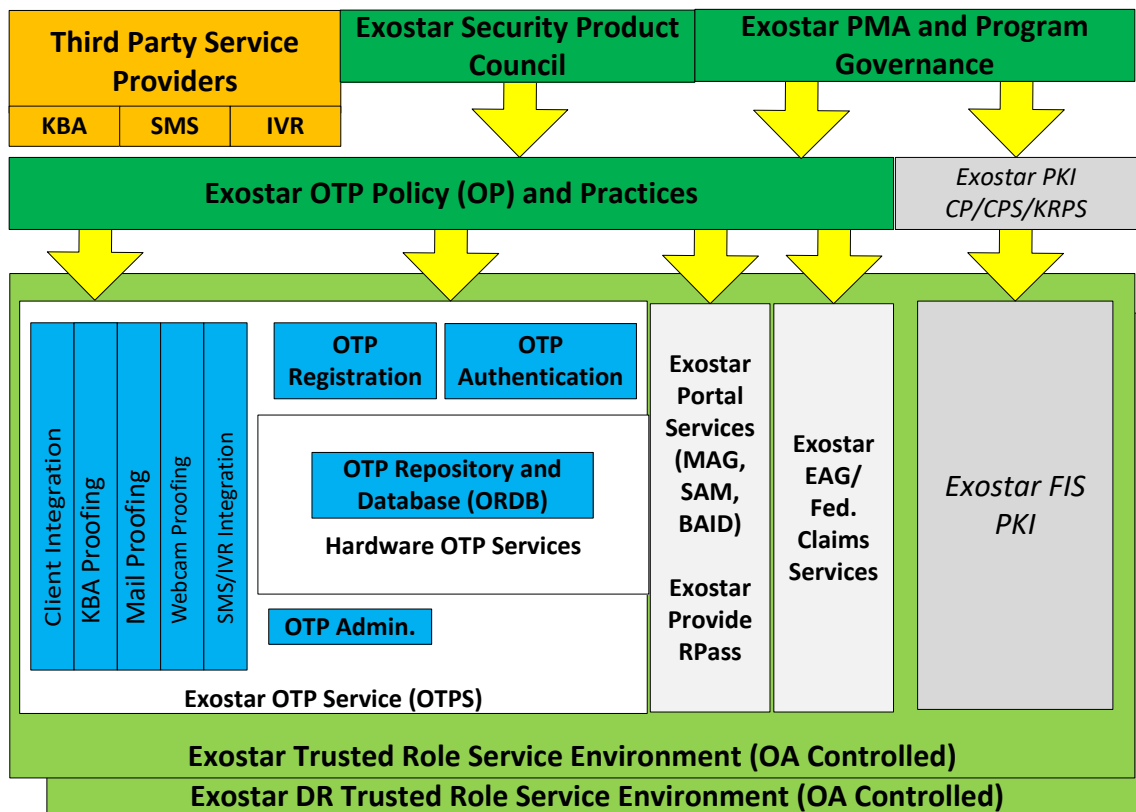
This One-Time Password (OTP) Policy defines policies to facilitate interoperability between the Exostar OTP Service and relying party domains, using hardware-based OTP tokens, Short Message Service (SMS)-based OTP software tokens, Interactive Voice Response (IVR)-based OTP tokens, and software-based tokens provided (e.g. smartphone and tablet mobile device apps) via the Exostar Identity Federation.

Additionally, Exostar’s Identity Federation services accept Exostar and third-party issued Public Key Infrastructure (PKI) authentication credentials from approved digital certificate issuers, as described in the *Exostar FIS Certificate Policy*.

The word “assurance” used in this policy means how well a Relying Party can be certain of the identity binding between the OTP token and the individual during authentication.

Interoperability will be achieved through the use of Identity Federation standards.

This policy covers the Exostar OTP Service (OTPS), which is integrated with the Exostar Managed Access Gateway (MAG), Exostar Secure Access Manager (SAM), Boeing Aviation ID (BAID), Exostar ProviderPass, and Exostar Enterprise Access Gateway (EAG) services. These services are operated under the governance of the Exostar PMA and Exostar Security Program. Any use of or reference to this policy outside the purview of the Exostar Identity Federation is completely at the using party’s risk.



Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

This policy is written to support relying party and interoperability objectives, as outlined in the Initiative for Open Authentication (OATH) Reference Specification.

1.1 Overview

1.1.1 One-Time Password Policy (OP)

This OP is established by the Exostar PMA as a policy under which all OTP service operations will be performed, and to provide a basis for Relying Party organizations to make their own risk determinations regarding the strength and suitability of Exostar OTP service assertions.

1.1.2 Relationship between this Policy and the OTP Practices Statement (OPS)

This OP provides stipulations for the implementation and operation of the Exostar OTP service. For certain high-sensitivity and proprietary functions, implementation detail may be redacted and addressed in separate Exostar OTP Practices Statements (OPS) which may be defined at the discretion of the Exostar PMA.

1.1.3 Scope

The scope of this OP includes all Exostar OTPS components, including the OTP Registration (OReg), OTP Authentication (OAuth), OTP Administration (OAdm), OTP Repository and Database (ORDB), OTP Client integration, Remote Proofing Services (RPS), Short Message Service (SMS), Interactive Voice Response (IVR), Mobile Device App-based Credentials, and Video Proofing functions.

The OP also addresses certain supporting elements of MAG, EAG, SAM, BAID, and ProviderPass, in which Exostar-issued OTP credentials are utilized.

1.2 Federation Participants

1.2.1 Authorities

1.2.1.1 Exostar Security Product Council (ESPC)

The ESPC is responsible for:

- Providing customer business and security input regarding the Exostar Managed Access Gateway (MAG), Enterprise Access Gateway (EAG), and the Exostar OTP Service.
- Reviewing, assessing, and accepting the security controls applied to each of these services.

1.2.1.2 Exostar PMA

The Exostar PMA, whose membership includes the Exostar Security Program and Product Managers, is responsible for:

- Governance and oversight of the Exostar OTP Service,
- Drafting and approval of the Exostar OP,
- Drafting, analysis, and approval of the supporting OPS (where applicable), and

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

- Coordinating communications with Relying Parties to the MAG, EAG, SAM, ProviderPass, and OTP Service.

1.2.1.3 Exostar Operational Authority (OA)

The Exostar OA is the group responsible for operation of the Exostar MAG, EAG, SAM, ProviderPass, and OTP services, under oversight by the Exostar PMA.

1.2.1.4 Exostar Operational Authority Administrator (OAA)

The Exostar Operational Authority Administrator is responsible for the management, availability, and day-to-day operational security of the Exostar MAG, EAG, SAM, ProviderPass, and OTP services. The OAA serves as the head of the Exostar OA and is appointed by the Exostar PMA.

1.2.1.5 Exostar Security Office

The Exostar Security Office is responsible for internal audit administration and oversight of the Exostar OA's compliance with Exostar MAG, EAG, SAM, ProviderPass, and OTP service controls.

1.2.1.6 Subscriber Organization Sponsor

The Subscriber Organization Sponsor is responsible for purchase and distribution of an OTP Token to an individual Subscriber user within their organization.

1.2.1.7 Token Vendor

The Token Vendor is responsible for OTP hardware token manufacture and, optionally, token initialization processes.

1.2.1.8 RPS Provider

The Remote Proofing Service (RPS) Provider is responsible for service components which pin and proof user identities using out-of-wallet questions. These services may be hosted and managed separately from Exostar's core identity management services.

1.2.1.9 SMS Provider

The Short Message Service (SMS) Provider is responsible for service components which transmit one-time passcodes to end users' telephonic devices by SMS or text message. These services may be hosted and managed separately from Exostar's core identity management services.

1.2.1.10 IVR Provider

The Interactive Voice Response (IVR) Provider is responsible for service components which deliver one-time passcodes to end users' telephonic devices by voice call. These services may be hosted and managed separately from Exostar's core identity management services.

1.2.1.11 Mobile Device App (APP) Provider

The Mobile Device App Provider is responsible for service components which manage enrollment and authentication functions of end users' mobile applications. Authentication may occur in several modes including authentication of OATH TOTP's generated by the app-based software token, or online via a "push notification" style authenticator, both of which prove the end user's possession of the mobile device.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

1.2.2 Exostar Identity Management Services**1.2.2.1 Exostar Managed Access Gateway (MAG) Service**

Exostar MAG provides a structured Identity Provider (IdP) service, within which Subscriber Organizations, individual Subscribers, and their respective attributes are maintained for use within the Identity Federation. MAG is designed primarily for the Aerospace and Defense supply chain.

1.2.2.2 Exostar Enterprise Access Gateway (EAG) Service

Exostar EAG provides a mechanism for Subscriber Organizations to maintain their own Identity Provider (IdP) repositories and to utilize them as part of the Exostar Identity Federation.

1.2.2.3 Exostar One Time Password Service (OTPS)

The Exostar OTPS provides a mechanism for Subscriber Organizations and individual Subscriber users to bind their identities to hardware-based HOTP tokens or registered telephone numbers, for use as a second factor in the Exostar Identity Federation. (In runtime use, the MAG, EAG, SAM, or ProviderPass services provide identity and first-factor authenticators.)

The OTPS is composed of the following major components:

- OTP Registration, which provides a binding of Exostar MAG Subscribers to assigned OTP Service hardware tokens
- OTP Authentication, which provides multi-factor user login and is Internet-accessible via the Exostar MAG service
- OTP Administration, which includes token file provisioning and release management and is accessed from Exostar's internal Trusted Role server interfaces
- OTP Repository and Database, which provides protected storage of Subscriber user identity and token bindings
- OTP Client Integration API, which provides an automated integration point to Exostar's RPS, SMS, and IVR components
- Remote Proofing Service (RPS) integration, which provides questions from publicly available or proprietary databases to enable proofing of Subscribers
- Video Proofing services, which allow an alternative, webcam-based video proofing of Subscribers
- Short message service (SMS) integration, which provides Subscribers the ability to register and use an SMS-enabled device for second-factor authentication to the OTP Authentication component
- Interactive Voice Response (IVR) service integration, which provides Subscribers the ability to use Exostar two-factor authentication without an SMS-enabled device or hardware token

1.2.2.4 Exostar Federated Identity Service (FIS)

Exostar FIS provides public key infrastructure (PKI) and related certificate services to Subscriber Organizations. Exostar FIS is governed and managed by the Exostar PMA and OA separately from the Exostar OTP Service.

1.2.2.5 Exostar Secure Access Manager (SAM)

Exostar SAM provides a structured Identity Provider (IdP) service, within which Subscriber Organizations, individual Subscribers, and their respective attributes are maintained for use within the Identity Federation. SAM is designed primarily for the Life Sciences industry.

1.2.2.6 Exostar ProviderPass

Exostar ProviderPass is an API-based Web Service, which provides Exostar clients operating Electronic Health Record (EHR) systems with identity verification, second-factor issuance and

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

authentication, and electronic prescription digital signing for healthcare providers writing Electronic Prescriptions for Controlled Substances (EPCS).

1.2.2.7 Boeing Aviation ID (BAID)

BAID provides a structured Identity Provider (IdP) service, within which Subscriber Organizations, individual Subscribers, and their respective attributes are maintained for use within the Identity Federation. SAM is designed primarily for the Aerospace customer (e.g. airline) community.

1.2.3 Participants

1.2.3.1 Subscriber Organizations

Organizations who subscribe to the Exostar OTP Service, as part of their utilization of the Exostar MAG, EAG, SAM, or ProviderPass services, are considered Subscriber Organizations within the scope of this OP.

1.2.3.2 Subscribers

Individual end users who are affiliated with Subscriber Organizations are considered Subscribers within the scope of this OP.

1.2.4 Relying Parties

A Relying Party is an organization that relies on the validity of the binding of the Subscriber's name to an OTP token (Token) and IdP account. The Relying Party is responsible for deciding whether to accept the Token's binding to an individual Subscriber.

1.2.5 Applicability

1.2.5.1 Obtaining Tokens

OTP hardware tokens shall be distributed by Exostar and registered for use by a specific Subscriber Organization and individual Subscriber user. OTP Registration shall provide a binding of the token's owner to their Identity record in the Exostar MAG, SAM, BAID, or ProviderPass service.

This stipulation does not apply to the SMS,IVR, APP authentication methods.

1.3 Token Usage

1.3.1 Appropriate Token Uses

OTP tokens shall be utilized by Subscriber Organizations and individual Subscribers for purposes of authenticating to the Exostar MAG, SAM, BAID, or ProviderPass services.

1.3.2 Prohibited Token Uses

OTP tokens shall not be used in unapproved application interactions or by Subscribers to which they were not assigned during OTP Registration.

1.4 Policy Administration

1.4.1 Organization administering the document

The Exostar PMA is responsible for all aspects of this OP and may from time to time revise, extend, or amend this policy subject to the approval procedures defined herein and as specified in applicable relying party agreements.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

1.4.2 Contact Person

Questions regarding this OP shall be directed to the Chair of the Exostar PMA.

1.4.3 Person Determining OP and OPS Suitability

The Exostar PMA shall determine the suitability of this OP and additional OPS details.

1.4.4 OP and OPS Approval Procedures

THE OP AND OPS ARE SUBJECT TO AMENDMENT BY THE EXOSTAR PMA IN ACCORDANCE WITH THE PROCEDURES SET FORTH HEREIN.

The Exostar PMA shall review and approve the OP, and optionally one or more OPS documents, including all proposed revisions, modifications and amendments. All such revisions, modifications and amendments shall be recorded in the minutes of the Exostar PMA.

Proposed revisions, modifications and amendments to the OP and the security controls described herein shall be distributed to members of the Exostar Security Product Council (ESPC) for comment, with not less than 30 days' notice, prior to the effective date of proposed such revisions, modifications and amendments. Notwithstanding the foregoing, the Exostar PMA shall make all final determinations, in its sole discretion, regarding all revisions, modifications and amendments to the OP and OPS.

1.4.5 Waivers

Waivers to the OP may be issued by the ESPC, which represents all relying parties.

2 PUBLICATION & REPOSITORY RESPONSIBILITIES

2.1 Public Repositories

No public repository of OTPS Subscribers or Subscriber tokens shall be established.

A private repository of Subscriber identities may be created. If so, it shall be restricted to Subscriber Organizations and authorized administrative personnel.

2.2 Authoritative Private Repositories

For hardware tokens, an authoritative OTP Repository and Database (ORDB) shall be established and managed by Exostar under the controls defined in this OP.

For identities bound to SMS- and IVR-based authenticators, the Exostar database shall be authoritative.

For Identities bound to APP-based authenticators, the Exostar database shall bind the identity to a unique and immutable identifier within the APP provider's database, together which shall be deemed authoritative.

2.3 Repository Obligations

Exostar shall maintain the confidentiality and integrity of all repository information under its control.

Such information may be utilized in authorized Trusted Role administrative functions, may be provided to authorized Subscriber Organization data owners via secure mechanisms, and may be included in Identity Federation assertions and provisioning transactions within the production operational environment. However, operationally sensitive information (e.g. token secrets) shall not be distributed.

Integrity and confidentiality of repository information within the APP vendor's database shall be maintained in accordance with industry best practices and contractual obligations with Exostar. This data is not considered PII, comprising only end users' email addresses, mobile device telephone numbers, and authentication event history, which for "push" authentications may include contextual information sent to the APP vendor by Exostar.

2.4 Access Controls on Repositories

Administrative access to the ORDB and other Exostar production databases (e.g. MAG, SAM, ProviderPass, BAID, SOTP) shall be controlled as an Exostar Trusted Role function.

Runtime access to the ORDB, including programmatic access to Subscriber account and token key information shall be conducted exclusively from servers within Exostar's production Trusted Role environment.

Critical Subscriber and token key information, including personally identifiable information (PII) shall be encrypted when in transit across untrusted networks and at rest in Exostar's Trusted Role database.

Access to ORDB encryption information shall be protected as defined in section 6.5.

As APP vendor databases do not contain PII, these databases need not be TR controlled.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

3 IDENTIFICATION & AUTHENTICATION

The Exostar MAG, SAM, BAID, ProviderPass, and Identity Federation services utilize a range of policy labels which are aligned with US Government standards, including US NIST Special Publication 800-63 and OMB-04-04. A mapping of Exostar's policy labels to these standards is maintained in support of this policy.

Exostar policy labels provide flexibility in meeting both US Government-aligned standards and industry-specific Commercial Best Practice ("CBP") requirements. These labels are based on a combination of authenticator strength and identity proofing processes, and Exostar shall provide each relying party in the Exostar Identity Federation with granular attribute information as part of the Identity Federation claim.

Exostar Policy Label "Level 3":

Authenticator – Exostar Hardware OTP or APP (Level 3)

Proofing Process – Exostar RPS, mail, and webcam proofing (Level 3)

Exostar Policy Label "Level 3 CBP" – Option A:

Authenticator – Exostar Hardware OTP or APP (Level 3)

Proofing Process – Commercial Antecedent Relationship (Level 3 CBP)

Exostar Policy Label "Level 3 CBP" – Option B:

Authenticator – Exostar SMS/IVR (Level 3 CBP)

Proofing Process – Exostar RPS, mail, and webcam proofing (Level 3)

Depending on specific customer and Subscriber requirements, one or more of the following components may be implemented by a Subscriber Organization as part of the Exostar Identity Federation:

- Identity Proofing may be conducted by a Subscriber Organization or a Relying Party organization, in a delegated model similar to Registration Authority or Trusted Agent delegation in a PKI issuance model.
- Registration and Identity Proofing requests may be made by a Subscriber Organization using Exostar's Client Integration API.
- Authentication claims may be made by a Subscriber Organization using Exostar's EAG or similar integration to the Exostar Identity Federation.

In all such instances, the requirements and obligations of this Policy applicable to the locally implemented services shall flow-down to the Subscriber Organization.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

3.1 Naming

3.1.1 Types of Names

Exostar MAG, SAM, BAID, ProviderPass, and OTPS inherit Subscriber Organization and Subscriber name forms as identified in the Exostar PKI Certificate Policy. Additional name forms may be defined as described in the OPS.

3.1.2 Need for Names to be Meaningful

Subscriber Organizations shall be uniquely identified in the Exostar MAG, SAM, and BAID systems. ProviderPass Subscriber Organizations shall be at least as granular as the EHR vendor customer, but may include more granularity such as the healthcare provider organization.

Subscriber Organizations shall be bound by Exostar service agreements prior to utilizing Exostar MAG, EAG, SAM, BAID, ProviderPass, or OTPS.

Subscriber user accounts shall be uniquely identified in the Exostar MAG, SAM, BAID, and ProviderPass systems, and shall be linked as affiliates of a Subscriber Organization.

Subscriber user accounts shall not be shared among individuals.

3.1.3 Recognition, Authentication & Role of Trademarks

No stipulation.

3.1.4 Name Claim Dispute Resolution Procedure

The Exostar PMA shall resolve any name collisions brought to its attention that may affect interoperability or the integrity of Subscriber identity assertions.

3.2 Initial Identity Validation

3.2.1 Method to Establish Exostar MAG Account

Subscriber Organizations shall be established in the Exostar MAG, SAM, BAID, or ProviderPass system using established manual, automatic, and bulk load registration processes.

Subscriber users shall be established in the Exostar MAG, SAM, BAID, or ProviderPass system using established manual, automatic, and bulk load registration processes.

3.2.2 Authentication of Organization Identity

Subscriber Organizations shall accept Exostar's online Terms and Conditions and Service Agreements prior to utilizing the MAG, EAG, SAM, BAID, or OTP services. MAG and SAM Subscriber Organizations shall be identified by business contact information which includes one or more authorized Organization Administrators, who are identified by email addresses that are bound to the Subscriber Organization MAG record. ProviderPass subscribers individually accept Exostar's online Terms and conditions and Service Agreements prior to use.

Subscriber Organization Administrators shall initially authenticate themselves using a single-use password that is transmitted by Exostar MAG, SAM, or BAID to their registered email address. Subsequently, they shall change their single-use password to a permanent password over a TLS-protected channel.

3.2.3 Authentication of Individual Identity

Subscriber users are identified by business contact information, which includes a business email address that is bound to the Subscriber Organization MAG, SAM, or BAID record. Subscriber

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

users shall initially authenticate themselves using a single-use password that is transmitted by Exostar MAG, SAM, or BAID to their registered email address. Subsequently, they shall change their single-use password to a permanent password over a TLS-protected channel and authenticate using a password or combination of credentials that has been bound via this initial email process.

3.2.3.1 Human Subscriber Re-Authentication

Following recovery from a lost or compromised credential, Subscriber users shall re-authenticate to the Exostar MAG, SAM, or BAID service based on a single-use password that is transmitted to their registered email address and change their single-use password to a permanent password over a TLS-protected channel, or via in-person antecedent relationship with their Subscriber Organization Administrator.

3.2.3.2 Human Subscriber Initial Identity Proofing Via Antecedent Relationship

When explicitly permitted by Exostar, subscriber users may be proofed by Exostar via antecedent relationships in support of the OTP service, or by Subscriber Organizations at Level 3. Additionally, Subscriber Organizations may elect to utilize antecedent relationships in authenticating their own Subscriber users at Level 2.

3.2.4 Identification and Authentication for OTP Re-Sync Requests

For hardware tokens, Subscriber user token re-synchronization attempts shall be authenticated by a minimum of single-factor user ID and password authentication to the Subscriber's MAG, SAM, BAID, or ProviderPass account. Following MAG, SAM, BAID, or ProviderPass authentication, the Subscriber user shall establish possession of their registered hardware token through a protected online session.

3.2.5 Authentication for Level 3 Proofing

3.2.5.1 Level 3 Identity Binding via Remote Proofing Services

A Subscriber shall authenticate using an active MAG, SAM, or ProviderPass user ID/password credential prior to accessing the Level 3 RPS service. Additional authentication information shall be collected by the RPS as part of the remote proofing process, as described in Section 4.10.

3.2.5.2 Level 3 Identity Binding via Postal Delivery

A Subscriber shall authenticate using an active MAG, SAM, or ProviderPass user ID/password credential prior to requesting postal or mail delivery of a one-time use activation code.

3.2.5.3 Level 3 Identity Binding via Video Proofing

A Subscriber shall authenticate using an active MAG, SAM, or ProviderPass user ID/password credential prior to requesting video-based proofing. A credential of equivalent strength shall be used to authenticate the Subscriber at the beginning of the video proofing event.

3.2.5.4 Level 3 'Upgrade'

A Subscriber possessing a new or currently valid credential which has been bound at through an organization's antecedent may programmatically rebind the credential at Level 3 using the RPS, Postal Delivery, or Video Proofing processes after authenticating with the existing Level 2 credential.

An inactive, previously bound, or incorrectly bound Level 2 OTP Hardware token shall not be bound using the Level 3 'Upgrade' process.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

3.2.6 Identification and Authentication for Credential Reactivation after Revocation

Once revoked, a Subscriber user's OTP hardware token cannot be reactivated.

After a Subscriber user's OTP hardware token revocation, a single-use password shall be automatically sent by the MAG, SAM, or BAID system to the Subscriber's registered email address. The Subscriber shall then create a new password using a TLS-protected channel.

Authentication then shall be conducted by a minimum of single-factor user ID and password authentication to the Subscriber's MAG, SAM, or BAID account.

The stipulations of this section do not apply to SMS, IVR, or APP credentials, as phone numbers and APP IDs may be rebound after revocation provided the Subscriber user completes identity verification again as if registering for the first time.

3.3 Identification and Authentication for Revocation Request

A Subscriber Organization Administrator may authenticate to the Exostar MAG, SAM, or BAID service using either their single-factor (user ID/password) or two-factor (user ID/password and OTP token code) credentials for purposes of filing an OTP token revocation request for themselves or a Subscriber within their organization.

A Subscriber Credential Administrator may authenticate to the SAM service using either their single-factor (user ID/password) or two-factor (user ID/password and OTP token code) credentials for purposes of filing an OTP token revocation request for themselves or a ProviderPass Subscriber user of their EHR system.

An individual Subscriber user may authenticate to the Exostar MAG, SAM, or BAID service using their single-factor (user ID/password) credentials for purposes of filing an OTP token revocation request for their own token.

An individual Subscriber user may authenticate to the ProviderPass client EHR system using their single-factor (user ID/password) credentials for the purposes of filing an OTP token revocation request for their own token.

Exostar Customer Service personnel may initiate a revocation request on behalf of any Subscriber Organization Administrator or Subscriber user, based on an authenticated telephone, email, or web-based support case.

When token revocation occurs, an email notification will be sent to both the Subscriber and to the Subscriber Organization administrators. In addition, a single-use password may be sent to the Subscriber as described in Section 3.2.6.

3.4 Identification and Authentication for Credential Replacement

A Subscriber who has a valid Level 3 proofing on record in the OTPS database shall authenticate to the MAG, SAM, BAID, or ProviderPass service using OTP Hardware, SMS-based, IVR-based, or APP-based mechanisms prior to requesting or binding an alternate authentication device to their identity.

Such bindings shall not be requested or authorized by any other party or mechanism at Level 3. In the event that a Subscriber cannot authenticate using a Level 3 two-factor mechanism, the individual shall be required to re-establish control of the account and complete a new Level 3 proofing process prior to binding a new device to the identity.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

Loss or compromise of an active second-factor devices shall be addressed via a Revocation Request, as defined in Section 3.3.

3.5 Subscriber Assertion of US Person Status

A Level 3 MAG Subscriber, at their option, may submit documentation to Exostar asserting their US Person status, as defined by the US International Traffic in Arms Regulations (“ITAR”), using an out-of-band and auditable procedure (e.g. fax to an Exostar Registration Authority).

Exostar does not make any inquiry or investigation into any such assertion(s) and accepts it as presented. Such assertions shall include the Subscriber’s MAG user identifier or other unique identifier as directed by Exostar.

If the Subscriber provides such an assertion, the Subscriber’s US Person status shall be recorded in the MAG database record. Assertions of US Person status are representations of the Subscriber and not evidence of any investigation by Exostar.

4 CREDENTIAL LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Subscriber Organization Application

Subscriber Organization applications for the Exostar OTP service shall be performed within the authenticated and secured Exostar MAG, SAM, or BAID web interface, or via an Exostar MAG, SAM, or BAID bulk load process. ProviderPass Organization Applications shall be similarly managed by the ProviderPass client.

4.1.1 Submission of Credential Application to Exostar

Subscriber Organization token provisioning requests shall be submitted via the Exostar MAG, SAM, or BAID web interface, or a bulk load process, and shall be fulfilled via Exostar MAG, SAM, or BAID, and CRM systems. ProviderPass token provisioning requests shall be submitted by the ProviderPass client via the OTPS and CRM APIs.

4.1.2 Enrollment Process and Responsibilities

Subscriber Organizations shall designate one or more individual MAG, SAM, or BAID users as Subscriber Organization Administrators. ProviderPass clients shall designate one or more individual Credential Administrators.

4.2 Hardware Token Production and Shipment

Hardware tokens for the Exostar OTP service shall be initialized and shipped by Exostar or a known and trusted third party provider that is located in the United States, or from a country and locale that are approved in advance by the ESPC, using a controlled and audited process. In no circumstance will Subscriber Organization information be provided to the Hardware Token Vendor.

If token production is not performed by Exostar, specific production controls shall be specified in vendor contract terms.

Token initialization systems shall not be connected to the Internet or general vendor corporate networks.

To the greatest extent possible, token production systems should be hardened according to Specialized Security Limited Functionality (SSLF) usage profiles and aligned with the US Federal Desktop Core Configuration (FDCC) or equivalent standards.

The use of USB tokens and removable media on vendor production systems shall be limited to known and trusted devices through procedural and technical controls, and restricted to use cases which are critical to the operation of the token production facility.

Email, instant messaging, and web clients shall not be installed on any controlled token production system. Consideration shall be given to covert channels and single-party insider threat in vendor contracts, and production procedures shall be implemented which are commensurate with the Internet threat environment and known risks to the HOTP industry.

4.2.1 Hardware Token Production and Key Handling

OTP hardware tokens shall be manufactured and configured using the controls described in Section 4.2 above.

Token keys shall be generated in a hardware storage module using an HOTP algorithm that is consistent with RFC 4226. These keys may be persisted in plain text temporarily outside of the HSM only on vendor card production systems and shall not be retained by the hardware token vendor.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

4.2.2 Hardware Token Shipment

Hardware token shipment shall be conducted using a commercial shipment service. Verifiable delivery mechanisms shall be utilized where practical.

4.2.3 Hardware Token Seed File Delivery to Exostar

Key material for each production batch of OTP hardware tokens shall be managed by Exostar under Trusted Role controls. Provisioning file encryption methods and handling procedures shall be described in the Exostar OPS or comparable procedure.

4.2.4 Hardware Token Seed File Management

Once token seed files have been received by Exostar, the vendor shall delete all copies of the provisioning file and corresponding encryption material.

After token seed files have been processed by Exostar, copies of the provisioning file and corresponding encryption key material shall not be archived. All other copies shall be deleted from Exostar OTP production and supporting systems.

4.3 Subscriber Credential Application**4.3.1 Submission of Credential Application to Exostar**

Subscriber Organizations shall submit credential provisioning requests to Exostar via an authenticated and protected online session.

4.3.2 Enrollment Process and Responsibilities

Subscriber MAG and SAM Organization Administrators, or ProviderPass Client administrators, shall be responsible for enrolling their organization's shipping locations and points of contact for the OTPS, for correct use of the OTP Registration process, and for timely revocation of Subscriber user credentials following their loss, theft, or compromise.

The Subscriber Organization's responsibilities under this section shall extend to all forms of two-factor authentication devices, including loss or compromise of Subscriber and third party mobile devices, telephony equipment, and changes to active telephone numbers.

4.4 Level 2 Credential Application Processing**4.4.1 Performing Identification and Authentication Functions**

Subscriber MAG, SAM, and BAID Organization Administrators, and ProviderPass Credential Administrators shall be initially provisioned by Exostar using single-factor authentication as described in Section 3.2.2. OTP Registration privileges shall be activated after OTP services are enabled for the Organization.

4.4.2 Approval or Rejection of Credential Applications

Subscriber Organizations and individuals acting on behalf of Subscriber Organizations may apply to purchase OTP credentials directly from an Exostar e-commerce web site or through alternate channels defined by Exostar.

With the exclusion of commercial payment information, personally identifiable information shall not be collected as part of the OTP credential application; Subscriber and individual registration

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

information shall be collected as part of OTPS account activation and OTP token binding, as described in Section 4.6.

Upon receipt of payment, OTP credential applications will be approved for distribution and will be shipped to the purchaser's designated shipping address as defined in Section 4.2.2.

OTP credential applications may be rejected at Exostar's discretion. Reasons for application rejection may include, but are not limited to, failure of the purchaser or shipping location to meet commercial or legal obligations, such as an entity's inclusion in a government-defined denied parties list.

Approval and shipment notifications will be sent to purchasers through Internet email.

4.4.3 Time to Process Credential Applications

Processing and activation of OTP Credentials shall be completed within 30 days of submission to Exostar.

4.5 Credential Issuance

The OTPS serves as both the credentialing Registration Authority (RA) system and the Identity Provider (IdP) for Exostar OTP token Subscribers.

Exostar-initialized OTP hardware tokens shall be issued to applicants based on the commercial purchase and shipment controls described in Section 4.4.2 and 4.2.2, respectively. SMS, IVR, and APP-based tokens shall be issued immediately to the Subscriber's telephone number upon registration.

Binding of the credential applicant to an established Subscriber Organization and Subscriber end user identity shall be conducted at the time of token activation, as described in Section 4.6.

4.6 Credential Activation

OTP credential activation shall be performed within the OTPS, by the Subscriber, or in the case of BAID, an authorized Subscriber Organization Administrator who is authenticated to the OTPS using an Exostar-issued OTP credential, Exostar Medium-Hardware credential, or equivalent credential.

4.6.1 Conduct Constituting Credential Acceptance

Subscriber authentication to the Exostar MAG, SAM, BAID, or ProviderPass service following completion of the OTP Registration process shall constitute acceptance of the credential and successful binding to the Subscriber's MAG, SAM, BAID, or ProviderPass account.

4.7 Hardware Token Replacement

4.7.1 Circumstance for Token Replacement

OTP tokens may be replaced by a Subscriber following token loss, compromise, or damage to an existing token.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

4.7.2 Who may Request Replacement

Subscriber Organizations and individuals acting on behalf of Subscriber Organizations purchase replacement OTP tokens.

4.7.3 Processing Token Replacement Requests

Token replacement shall be processed in the same manner as described in Section 4.4 for initial token provisioning.

4.7.4 Notification of New Token Issuance to Subscriber

Upon binding of a new OTP token to a user account, email notification shall be sent by the OTPS to the Subscriber end user's registered email address and to all registered administrators for the Subscriber Organization.

4.7.5 Conduct Constituting Acceptance of a Renewal Token

Subscriber authentication to the Exostar OTP service using the new hardware token following completion of the OTP Registration process shall constitute acceptance of the hardware token and successful binding to the Subscriber's OTPS account.

4.8 Hardware Token Re-Sync**4.8.1 Circumstance for Token Re-Sync**

Time-based and event-based OTP hardware tokens may fail to properly synchronize with the OTPS from time to time. A Subscriber user token re-synchronization feature shall be provided to address such issues.

4.8.2 Who may Request Token Re-Sync

A Subscriber user who is in possession of their hardware token may request token re-synchronization.

A Subscriber user who is in possession of their hardware token, an authorized Subscriber Organization Administrator or Credential Administrator, or an Exostar OTP Administrator may unlock a Subscriber user account in support of token re-sync.

4.8.3 Processing Token Re-Sync Requests

Token re-synchronization requests shall be conducted via an authenticated and SSL/TLS-protected session in the OTP Authentication web interface.

4.8.4 Notification of Token Re-Sync to Subscriber

An email shall be sent to each MAG, SAM, or BAID Subscriber Organization Administrator (if applicable), or ProviderPass Credential Administrator, and the Subscriber user's registered email addresses following each successful token re-synchronization.

4.9 Credential Revocation and Suspension**4.9.1 Circumstance for Revocation of a Credential**

An OTP credential shall be revoked by the Subscriber Organization whenever a token is lost, stolen, or compromised, or when the token's binding to the individual Subscriber user becomes invalid.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

4.9.2 Who Can Request Revocation of a Credential

A Subscriber MAG, SAM, or BAID Organization Administrator, or a ProviderPass Credential Administrator may request revocation of any OTP credential issued under their organization's service agreement with Exostar.

A Subscriber user may request revocation of their own OTP credential.

Exostar Officers may request revocation of OTP credentials on behalf of any Subscriber Organization Administrator or Subscriber user, based on an authenticated telephone, email, or web-based support case.

4.9.3 Procedure for Revocation Request

OTP credential revocation requests shall be submitted through a protected online session.

Authenticated revocation requests shall be effective upon submission to the Manage OTP web application.

4.9.4 Revocation Request Grace Period

Revocation shall be submitted in a timely manner following a Subscriber's detection of loss, theft, or compromise. Once revoked, OTP hardware tokens may not be re-used or re-activated as part of the Exostar OTP service.

4.9.5 Time within which Exostar must Process the Revocation Request

Revocation requests shall be processed in a timely manner following submission to the Manage OTP system.

4.9.6 Circumstances for Credential Suspension

An OTP credential may be suspended by the Subscriber Organization whenever a device is inaccessible or temporarily unavailable for use in conjunction with a Subscriber's MAG, SAM, BAID, or ProviderPass account, provided that there is no identified risk of theft or compromise.

4.9.7 Who can Request Credential Suspension

A Subscriber Organization Administrator may request temporary suspension of any OTP credential issued under their organization's service agreement with Exostar.

A Subscriber user may request temporary suspension of his/her own OTP credential.

4.9.8 Procedure for Credential Suspension Request

OTP credential suspension requests shall be submitted through a protected online session.

Authenticated suspension requests shall be effective upon submission to the Manage OTP web application.

Following temporary suspension of a Subscriber's credential, mechanisms shall be implemented to convey reduced or alternate authentication mechanisms to Relying Parties (fallback to single-factor password authentication, use of an alternate token or device, etc.).

Such temporary authentication mechanisms shall incorporate risk scoring attributes as described in the OPS.

4.9.9 Limits on Credential Suspension Period

OTP credentials shall not be suspended for more than 30 days. Beyond this period, credential status shall be changed to 'permanently revoked'.

4.10 Level 3 Remote Proofing Service

4.10.1 Application

Following single-factor authentication to Exostar MAG, SAM, BAID or a ProviderPass client as described in Section 3.2.5, an Applicant for Level 3 identity binding shall be directed to the RPS identity pinning and proofing workflow. The application shall be delivered via an SSL/TLS protected session between the Applicant and the Exostar OTP service.

Personally Identifiable Information (PII), including the Applicant's full legal name in combination with the individual's date of birth, home address, personal telephone number(s), and social security number or other government identifier(s) and identity document attributes may be collected as part of the Level 3 RPS application.

All PII collected by this workflow shall be securely forwarded to the RPS Provider for processing as described in Section 4.10.2. If applicable, this information shall be encrypted at rest and shall not be permanently stored on the Exostar OTP system.

If the Level 3 RPS processing is successfully completed, the RPS Provider shall return a positive response to the Exostar production system, and the OTPS database and audit history shall record the identity binding as a Level 3 Subscriber.

If Level 3 RPS processing cannot be completed successfully, the RPS Provider shall return a negative response to the Exostar production system and the OTPS database and audit history shall record the failure.

Following a Level 3 RPS failure, the Applicant:

- May retry Level 3 RPS processing up to a maximum number of attempts, which shall be defined by Exostar. Subsequent Applicant requests for Level 3 RPS processing shall be automatically rejected by the Exostar system.
- May request activation via Postal Delivery (Section 4.11) only for the address that is successfully matched and returned from the Level 3 RPS .
- May use Video-based proofing (Section 4.12).

4.10.2 Processing

Processing of the Level 3 RPS application shall occur between the Applicant and Exostar systems using server authenticated SSL/TLS, and between the Exostar system(s) and the RPS Provider system(s) using an SSL/TLS session.

The Level 3 RPS process shall include the following elements when processing:

- Applicant's legal name
- Applicant's date of birth
- Applicant's claimed home address
- All or a subset of the Applicant's social security number or other government identification number(s)
- Applicant's claimed home phone number

The Level 3 RPS process may include the following elements when processing:

- Applicant's mobile phone number
- Applicant's credit card number

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

- Applicant's credit bureau freeze PIN/password

During processing, the RPS Provider shall first 'pin' the Applicant's identity by matching this collected information to publicly available and/or proprietary database sources.

If the Applicant cannot be successfully pinned, the application shall be rejected by the RPS Provider (see Section 4.10).

If the Applicant is successfully pinned to an RPS Provider identity record, the Applicant shall proceed to Level 3 RPS knowledge-based proofing:

- The RPS Provider shall present the Applicant with a predetermined number of questions based on publically available and/or proprietary database sources, which shall not be re-used across the Applicant's Level 3 proofing process.
- A minimum number of correct responses, including a minimum number of correct responses to financial records-based challenge questions shall be established by the RPS.

If all of these proofing criteria are satisfied, the Subscriber shall provide:

- a) A telephone number of an SMS-enabled device;
- b) A telephone number for use in IVR-based authentication; or
- c) A telephone number for use in APP-based authentication; or
- d) If applicable, a Hardware OTP token serial number and two sequential OTP passcodes as proof-of-possession

For SMS/IVR OTP binding, the Exostar OTP service shall initiate initial SMS or IVR-based authentication to bind the Applicant to the Subscriber's selected telephone number. Upon receipt of the initial OTP token, the Applicant shall enter the OTP code received by the SMS or IVR mechanism within the same SSL/TLS session that was used to complete Level 3 proofing.

For Hardware OTP binding, the Subscriber shall demonstrate proof of possession of the token by authenticating to the Exostar MAG service within the same SSL/TLS session that was used to complete Level 3 proofing.

For APP binding, the OTPS sends the mobile phone number of the user to the APP service over a TLS session to the APP service API.

If the phone number is not already associated with an APP ID, the APP service sends an SMS to the phone number that includes a hyperlink to download the app.

The user clicks the hyperlink and installs the APP. The APP opens and begins the registration process with the APP service. The APP proves that the user controls the phone number, which is achieved via authentication of an OTP sent OOB via SMS or Voice to the phone number specified.

Following successful registration of the Subscriber's telephone number, APP, or Hardware OTP token, the Applicant shall be bound as a Level 3 Subscriber in the OTPS database.

If the Applicant does not successfully complete both Level 3 RPS processing and number/device registration during the same SSL/TLS session, Exostar MAG, SAM, BAID, or ProviderPass shall restart the registration and may direct the Applicant to re-execute RPS processing.

The Subscriber's US Person status shall not be set by Level 3 RPS proofing.

4.11 Level 3 Binding via Postal Delivery

4.11.1 Application

In the event that an Applicant completes identity pinning but cannot complete Level 3 RPS proofing as described in Section 4.10, the Applicant may select proofing via delivery of a one-time passcode that is delivered to the Applicant's address of record as delivered by the RPS and defined in section 4.10.1.

The application for activation via Postal Delivery shall be submitted by the Applicant following single-factor authentication to Exostar MAG, SAM, BAID, or ProviderPass as described in Section 3.2.5, using an SSL/TLS protected session.

4.11.2 Processing

The Level 3 activation via Postal Delivery process shall include the following elements based on earlier Level 3 RPS processing:

- Applicant's legal name
- Applicant's address of record as provided by the RPS
- A one-time passcode which is generated by Exostar OTP systems and is sent to the Applicant via postal channels, either by Exostar or a third party with commensurate controls.

The one-time passcode shall be a minimum of eight characters and shall be based on a pseudo-random number generator that is operated under Exostar Trusted Role control. The passcode shall be generated within Exostar OTPS and shall not be stored or written down, except within the Exostar databases and on the document which is sent to the Applicant. The passcode shall only be valid for a configured period of time.

Upon receipt of the one-time passcode, the Applicant shall initiate processing of the application via the Exostar OTP service.

Processing of Level 3 Binding via Postal Delivery shall be conducted between the Applicant and the Exostar OTP service using a single-factor authenticated SSL/TLS session, as described in Section 3.2.5.

If all of these proofing criteria are satisfied, the Subscriber shall provide:

- a) A telephone number of an SMS-enabled device; or
- b) A telephone number for use in IVR-based authentication; or
- c) A telephone number for use in APP-based authentication; or
- d) A Hardware OTP token serial number and one-time passcode as proof-of-possession.

For SMS/IVR binding, the Exostar OTP service shall initiate initial SMS or IVR-based authentication to bind the Applicant to the Subscriber's selected telephone number. Upon receipt of the one-time passcode, the Applicant shall enter the passcode received by the SMS or IVR mechanism within an SSL/TLS session.

For Hardware OTP binding, the Subscriber shall demonstrate proof of possession of the token by authenticating to the Exostar MAG or OTP service within an SSL/TLS session.

For APP binding, the OTPS sends the mobile phone number of the user to the APP service over a TLS session to the APP service API.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

If the phone number is not already associated with an APP ID, the APP service sends an SMS to the phone number that includes a hyperlink to download the app.

The user clicks the hyperlink and installs the APP. The APP opens and begins the registration process with the APP service. The APP proves that the user controls the phone number, which is achieved via authentication of an OTP sent OOB via SMS or Voice to the phone number specified.

Following successful registration of the Subscriber's telephone number, APP, or Hardware OTP token, the Applicant shall be bound as a Level 3 Subscriber in the MAG database.

If the Applicant does not provide a correct one-time passcode within a pre-configured number of attempts, the OTPS shall automatically reject the request.

The Subscriber's US Person status shall not be set by Binding via Postal Delivery.

4.12 Level 3 Video Proofing

4.12.1 Application

An Applicant may schedule Video Proofing in the event that they are not US based, opt-out of RPS Proofing, or cannot complete Level 3 RPS or Level 3 Binding via Postal Delivery.

Applications for Video Proofing shall be recorded in the SOTP system.

4.12.2 Processing

Exostar Level 3 Video Proofing shall be conducted by Exostar Trusted Role CA Officers, Trusted Role Video Proofer, or Trusted Agents ("Proofer") who are authorized and trained specifically to conduct Video Proofing.

Processing of Video Proofing applications shall be completed using a minimum of user ID and password on server authenticated SSL/TLS sessions.

Following submission, Exostar Trusted Role personnel shall schedule an interactive online proofing session with the Applicant using voice, email, or other out of band communications mechanisms.

Video proofing shall be conducted using technologies and processes which ensure the following:

- Trusted Registration Authority hardware and software shall be dedicated to identity proofing and approval functions, and shall be hardened and monitored to minimize the risk of malware or subversion of the registration process
- Applicant hardware and software shall be based on a commercially available and supported operating system
- Application anti-malware controls shall be the sole responsibility of the Applicant
- Both the Applicant's and the Exostar Registration Authority's systems shall support bi-directional, web-based video at 720p or higher resolution and audio feeds.
- Proofing shall utilize an individually authenticated and secure web-based conferencing session between the Applicant and the Exostar Registration Authority (e.g. WebEx or similar conferencing with strong, individually assigned user ID/passwords)
- Proofing shall provide sufficient resolution and clarity to ensure that Registration Authority personnel can identify readily identifiable forgeries or fabrications of common government-issued identity documents (i.e. able to determine the presence and validity of a raised seal or hologram)
- No recording or transcript of the Video Proofing event shall be created or retained by any party

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

The Proofer shall initiate a secure web conference with the Applicant, and shall conduct identity proofing using a documented proofing procedure.

Proofing criteria shall at minimum include the following items:

- The identity of the person performing the identity verification;
- A signed declaration by that person that he or she verified the identity of the subscriber as required by the applicable policy which may be met by establishing how the subscriber is known to the verifier as required by this Policy;
- The Applicant shall present one valid national government-issued photo ID or valid non-national government issued photo ID (e.g., driver's license, passport), which are issued by governments or international jurisdictions recognized by the US Federal Government.
- Unique identifying numbers from the identifier (ID) of the subscriber;
- The date and time of the verification; and
- A declaration of identity by the applicant and performed in the presence of the Proofer, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.
- Delivery of a one-time use passcode comprised of a minimum of 8 pseudo-random characters.

The Proofer shall not collect or record copies or images of the identity documents presented by the Applicant during the proofing event.

The Proofer shall record the results of the proofing event in an SSL/TLS protected OTPS session which is authenticated by Exostar Medium-Hardware PKI credentials.

Any collected information which includes Personally Identifiable Information presented by the Applicant shall be encrypted at rest in the Exostar database.

At the completion of the proofing procedure, the Proofer shall authenticate using a two factor credential and formally approve or reject the proofing event in the OTP system. If the proofing event is approved, the Proofer shall verbally provide the Applicant with a one-time passcode for use in the OTP system.

Upon receipt of the one-time passcode, the Applicant shall authenticate to the Exostar MAG, SAM, BAID, or ProviderPass service using a single-factor authenticated SSL/TLS session, as described in Section 3.2.5. The Subscriber shall provide a one-time use passcode that is delivered during the video proofing process and one or more of the following:

- a) A telephone number of an SMS-enabled device
- b) A telephone number for use in IVR-based authentication
- c) A telephone number for use in APP-based authentication;
- d) A Hardware OTP token serial number and two sequential OTP passcodes as proof-of-possession

For SMS/IVR binding, the Exostar OTP service shall initiate initial SMS or IVR-based authentication to bind the Applicant to the Subscriber's selected telephone number. Upon receipt of the one-time passcode, the Applicant shall enter the passcode received by the SMS or IVR mechanism within an SSL/TLS session.

For Hardware OTP binding, the Subscriber shall demonstrate proof of possession of the token by authenticating to the Exostar MAG or OTP service within an SSL/TLS session.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

For APP binding, the OTPS sends the mobile phone number of the user to the APP service over a TLS session to the APP service API.

If the phone number is not already associated with an APP ID, the APP service sends an SMS to the phone number that includes a hyperlink to download the app.

The user clicks the hyperlink and installs the APP. The APP opens and begins the registration process with the APP service. The APP proves that the user controls the phone number, which is achieved via authentication of an OTP sent OOB via SMS or Voice to the phone number specified.

Following successful registration of the Subscriber's telephone number, APP, or Hardware OTP token, the Applicant shall be bound as a Level 3 Subscriber in the MAG or OTP database.

4.13 Level 2 and 3 Authentication to MAG, SAM, BAID, and ProviderPass

OTP Subscriber authentication to MAG, SAM, BAID, ProviderPass, and the Identity Federation at Level 2 or Level 3 shall utilize a combination of Subscriber user ID and password managed by MAG, SAM, BAID or the ProviderPass client, plus one of the following second-factor authentication credentials. OTP Subscribers who have not completed identity proofing shall be authenticated at Level 2. OTP Subscribers who have completed identity proofing shall be authenticated at Level 3.

Subscriber authentication using Exostar-approved Level 4 PKI hardware credentials shall be accepted by the Identity Federation in lieu of these requirements.

4.13.1 OTPS Authentication

Hardware OTP tokens shall be authenticated by MAG, SAM, BAID, and ProviderPass using an SSL/TLS-protected user login page. Authentication shall be based on the Subscriber's provided MAG, SAM, or BAID user ID, password, and OTP token. ProviderPass clients shall authenticate Subscriber's user ID and password before directing the user to the OTPS. The Subscriber's account and Level 2 or Level 3 proofing status shall be verified against the authoritative database (Exostar OTPS).

4.13.2 SMS Authentication

Subscribers who use SMS-based tokens shall authenticate to MAG, SAM, BAID, or a ProviderPass client using an SSL/TLS-protected user login page. After the Subscriber enters their user ID and password, an SMS-based token of at least eight pseudo-randomized characters shall be sent by the Exostar production system to the Subscriber's registered phone number using an Exostar approved SMS Provider.

Communication between Exostar's production system and the SMS Provider shall be protected with a minimum of server authenticated SSL/TLS and authenticated by a service account and strong password.

The Subscriber's account and Level 2 or Level 3 proofing status shall be verified against the authoritative database (Exostar OTPS).

4.13.3 IVR Authentication

Subscribers who use IVR-based tokens shall authenticate to MAG, SAM, BAID, or a ProviderPass client using an SSL/TLS-protected user login page. After the Subscriber enters their user ID and password, an IVR-based token of at least eight pseudo-randomized characters shall be sent by the Exostar production system to the Subscriber's registered phone number using an Exostar approved IVR Provider.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

Communication between Exostar's production system and the IVR Provider shall be protected with a minimum of server authenticated SSL/TLS and authenticated by a service account and strong password.

Communication from the IVR Provider to Exostar's production systems may be permitted subject to a risk assessment and shall be protected by SSL/TLS.

The Subscriber's account and Level 2 or Level 3 proofing status shall be verified against the authoritative database (Exostar OTPS).

4.13.1 APP Authentication

APP-based authentication may occur in one of two modes as selected by the Subscriber.

4.13.1.1 TOTP Authentication

The user invokes the APP on the device, and obtains an OTP generated using the OATH TOTP algorithm with the device time +/- APP offset and **Token Seed** as inputs, or OATH HTOP algorithm with the counter index and **Token Seed** as inputs. After authenticating to MAG, SAM, BAID, or ProviderPass using his user ID and password, OTPS is invoked via UI or API and the user is prompted for a 6-8 digit OTP.

OTPS securely communications to the APP service using server authenticated SSL/TLS and API Key authentication, and provides the APP Service ID and OTP value to the APP Service. The APP service authenticates the OTP, and provides a response to OTPS within the same TLS session. TOTP codes are valid for 5 minutes to accommodate for time drift between the app time (device clock +/- sync Epoch) and server clock

4.13.1.2 OneTouch Authentication

After authenticating to MAG, SAM, BAID, or ProviderPass using his user ID and password, OTPS is invoked via UI or API and the user chooses to undergo "Push" authentication.

OTPS securely communications to the APP service using server authenticated SSL/TLS and API Key authentication, provides the APP ID, details of the transaction to be displayed by the app, a timeout interval x (set to 2 minutes), and requests that the APP service "OneTouch" authenticate the user. OTPS polls the APP service for a response. The APP service returns a UUID for this authentication transaction, and terminates the TLS connection.

The APP service will attempt to Push authenticate the user for the interval x .

The Push notification indicates that there are pending transactions. When the app is opened it syncs, thus requesting the pending transactions from the APP service. When the transaction is accept or denied, the app digitally signs the transition.

OTPS polls the APP service for up to interval x for a response for the request identified by the UUID.

The Subscriber's account and Level 2 or Level 3 proofing status shall be verified against the authoritative database (Exostar OTPS).

4.14 End of Subscription

Upon termination of a Subscriber user under an active Subscriber Organization, the Subscriber Organization Administrator or Credential Administrator shall disable the Subscriber user's account and revoke the corresponding hardware OTP token, APP, and/or SMS- and IVR-registered phone numbers.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

Once a Subscriber user account is revoked, a Subscriber Organization may not re-use a previously assigned hardware OTP token.

A telephone number may be re-used for APP-, SMS-, or IVR-based authentication provided that it is re-bound to a new Subscriber using the process in Section 4.10.

Upon termination of a Subscriber Organization's subscription to the Exostar MAG or SAM service, Exostar shall disable all accounts and login credentials (including OTP tokens) for the organization.

5 FACILITY MANAGEMENT & OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location & Construction

The location and construction of the facility housing OTPS equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the OTPS equipment and records.

5.1.2 Physical Access

5.1.2.1 OTPS Physical Access

OTPS equipment shall always be protected from unauthorized access. The physical security requirements pertaining to OTPS equipment are:

- Ensure no unauthorized access to the hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers
- Be manually or electronically monitored for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Provide at least three layers of increasing security such as perimeter, building, and server room
- Require two person physical access control to both the cryptographic module and computer system (Practice Note: Logical access is not multi-party controlled.)

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules shall be placed in secure containers.

A security check of the facility housing the OTPS equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”);
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

5.1.2.2 OTPS Administration Equipment Physical Access

OTPS administration equipment shall be protected from unauthorized access. The Exostar OA shall implement physical access controls to reduce the risk of equipment tampering and advanced physical threat vectors.

5.1.3 Power and Air Conditioning

The OTPS shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. OTP Authentication and ORDB components shall be provided with uninterrupted power sufficient for a minimum of 24 hours operation in the absence of commercial power, to support continuity of operations.

5.1.4 Water Exposures

The OTPS shall be housed in a facility that is protected against water exposures.

5.1.5 Fire Prevention & Protection

The OTPS shall be housed in a facility that is monitored for and protected against fire exposures (e.g. VESDA and zoned pre-action dry pipe systems).

5.1.6 Media Storage

OTPS media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit and / or archive information shall be stored in Exostar's Trusted Role archive, except when under review by an Exostar Audit Administrator. Backup information shall be stored at a site with physical, technical, and procedural controls commensurate to that of the operational OTPS.

5.1.7 Waste Disposal

Sensitive waste material (including hard drives, removable storage, tape media, and paper) shall be disposed of using a process that is aligned with the US NIST Special Publication 800-88 Moderate controls baseline.

a. Paper format:

- i. Shredding.
- ii. Burning.
- iii. Pulping.
- iv. Pulverizing.
- v. Rendered unreadable, and unable to be reconstructed

. b. Electronic format:

- i. Clearing i.e. using software or hardware products to overwrite media with non-sensitive data.
- ii. Purging i.e. degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains.
- iii. Destroying i.e. disintegration, pulverization, melting, incinerating, or shredding.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

5.1.8 Off-Site backup

Full system backups of the OTPS, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective OPS. Backups shall be performed not less than once every 7 days and stored off-site at a physical location at least 50 miles from the production site. At least one full backup copy shall be stored at an offsite location (at a location separate from the OTPS production equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical, technical, and procedural controls commensurate to that of the operational OTPS.

HA architecture shall not be construed as satisfying the above requirement for off-site backup. In circumstance of an HA deployment, the backup site shall be at least 50 miles from the nearest production site in the HA deployment.

All backups are encrypted using Exostar approved symmetric keys which are generated and maintained under two-person controls.

5.1.9 Third Party Facility Controls (RPS, SMS, IVR, and APP Providers)

Third party RPS, SMS, IVR, and APP service providers are not subject to specific Exostar facility controls requirements. Where applicable, these providers shall be commercially bound to protect confidential information, provide commensurate levels of information assurance, and to support audit inquiries related to Exostar OTPS operations.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role (Trusted Role) is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the OTPS is weakened. The functions performed in these roles form the basis of trust for all uses of the OTPS. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that malicious activity would require collusion.

The requirements of this policy are drawn in terms of four roles, which are consistent with those defined in the Exostar FIS and DCS Certificate Policy:

1. *Administrator* – authorized to install, configure, and maintain the OTPS; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
2. *Officer* – authorized to request or approve Tokens or Token revocations.
3. *Audit Administrator* – authorized to view and maintain audit logs.
4. *Operator* – authorized to perform system backup and recovery.

The following sections define these and other Trusted Roles.

5.2.1.1 Administrator

The administrator shall be responsible for:

- Installation, configuration, and maintenance of the OTPS;

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

- Establishing and maintaining OTPS system accounts;
- Configuring profiles or templates and audit parameters, and;
- Generating and backing up OTPS and Token keys.

Administrators may issue Tokens to Exostar Trusted Role personnel for use in support of the OTPS.

Administrators shall not issue Tokens to Subscribers.

5.2.1.2 Officer

For OTP Tokens, the Officer is responsible for the following activities:

- Registering new subscribers and requesting the issuance of Tokens;
- Requesting, approving and executing the revocation of Tokens;
- Performing Level 3 Identity Proofing;
- Initializing OTP hardware Tokens.

5.2.1.3 Audit Administrator

The Audit Administrator shall be responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the OTPS is operating in accordance with its OPS.

5.2.1.4 Operator

The operator shall be responsible for the routine operation of the OTPS equipment and operations such as system backups and recovery or changing recording media.

- May view and verify user and token information;
- May not add/change/delete user and token information.

5.2.2 Number of Persons Required per Task

A minimum of one person shall be required to perform the following tasks, which may be executed by third party manufacturing personnel, and who must be Trusted Roles subject to compliance with local laws:

- OTP hardware token key generation;
- OTP hardware token provisioning file generation and transmission.

Two or more persons shall be required to perform the following tasks:

- OTP hardware token seed file provisioning into the Exostar OTPS;
- OTP hardware token initialization;
- ORDB server private key generation, activation, and backup

Except for OTP hardware token initialization, where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a Trusted Role as defined in Section 5.2.1.

Multiparty control shall not be achieved using personnel that serve in the Auditor Administrator Role.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

All roles are recommended to have multiple persons in order to support continuity of operations.

5.2.3 Identification and Authentication for Each Role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

Except as specified elsewhere in this policy, Exostar-approved hardware OTP or PKI hardware tokens shall be utilized for authentication.

5.2.4 Roles Requiring Separation of Duties

Role separation, when required as set forth below, may be enforced either by the OTPS equipment, or procedurally, or by both means.

Individual OTPS personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, except:

- Individuals who assume an Officer role may not assume an Administrator or Audit Administrator role;
- Individuals who assume an Audit Administrator shall not assume any other role on the OTPS; and
- Under no circumstances shall any of the four roles perform its own compliance auditor function.

No individual shall be assigned more than one identity.

5.3 Personnel Controls**5.3.1 Qualifications, Experience, and Clearance Requirements**

A group of individuals responsible and accountable for the operation of each OTPS shall be identified. The Trusted Roles of these individuals per Section 5.2.1 shall be identified.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation. Personnel appointed to Trusted Roles shall:

- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere or conflict with their duties for the trusted role;
- Have not been previously relieved of duties for reasons of negligence or non-performance of duties;
- Have not been denied a security clearance, or had a security clearance revoked for cause;
- Have not been convicted of a felony offense; and
- Be appointed in writing by an approving authority.

For the Exostar OTPS, each person filling a Trusted Role shall satisfy at least one of the following requirements:

- The person shall be a citizen or permanent resident of the country where the OTPS is located; or

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

- The person shall have a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32

5.3.2 Background Check Procedures

All persons filling Trusted Roles, shall have completed a favorable background investigation per section 5.3.2 of the Exostar FIS and DCS Signing CA CPS.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the OTPS shall receive comprehensive training. Training shall be conducted in the following areas:

- OTPS security principles and mechanisms
- All software versions in use on the OTPS system
- All duties they are expected to perform
- Disaster recovery and business continuity procedures

Personnel receiving training shall acknowledge receipt and understanding of training material in writing.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles shall be aware of changes in OTPS operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

Job rotation should be conducted to the extent possible for all sensitive functions (e.g. system administration, database administration, network, and firewall administration).

5.3.6 Sanctions for Unauthorized Actions

The Exostar PMA shall take appropriate administrative and disciplinary actions against personnel who violate this policy.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to OTPS operations shall meet applicable requirements set forth in this OP (e.g., all requirements of Section 5.3).

Practice Note: Third party RPS, SMS, IVR, and APP service providers are not subject to this Exostar Trusted Role contractor requirement. Where applicable, these providers shall be commercially bound to protect confidential information, provide commensurate levels of information assurance, and to support audit inquiries related to Exostar OTPS operations.

5.3.8 Documentation Supplied To Personnel

The OTPS shall make available to its personnel the policies they support, the OPS, and any relevant statutes, policies or contracts. Other technical, operations and administrative documents (e.g., Administrator Manual, User Manual, etc.) shall be provided in order for the trusted personnel to perform their duties.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the OTPS. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 5.4.10.

5.4.1 Types of Events Recorded

All security auditing capabilities of the OTPS operating system, underlying operating systems (including applicable hypervisors, firmware, and hardware components) and the MAG, EAG, and OTP applications required by this OP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,
- The date and time the event occurred,
- Success or failure where appropriate,
- The identity of the entity and/or operator that caused the event,
- A message from any source requesting an action by the OTPS is an auditable event. The message must include message date and time, source, destination and contents.

The following events shall be audited:

Auditable Event	OTPS
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X
Any attempt to delete or modify the Audit logs	X
Obtaining a third-party time-stamp	X
Successful and unsuccessful attempts to assume a role	X
The value of <i>maximum number of authentication attempts</i> is changed	X
The number of unsuccessful authentication attempts exceeds the <i>maximum authentication attempts</i> during user login	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X
An Administrator changes the type of authenticator, e.g., from a password to OTP	X
The identity of the Proofing Agent	X
All security-relevant data that is entered in the system	X

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

Auditable Event	OTPS
All security-relevant messages that are received by the system	X
All successful and unsuccessful requests for confidential and security-relevant information	X
Whenever the OTPS generates a key (not mandatory for single session or one-time use symmetric keys)	X
The loading of OTPS private keys	X
All changes to the trusted OTP Public Keys, including additions and deletions	X
The manual entry of secret keys used for authentication	X
The export of private and secret keys (keys used for a single session or message are excluded)	X
All Token requests	X
All Token revocation requests	X
The approval or rejection of a Token status change request	X
Any security-relevant changes to the configuration of the Component	X
Roles and users are added or deleted	-
The access control privileges of a user account or a role are modified	-
Change of MAG, SAM, and OTP status (enabled, disabled, locked/unlocked) for a user's account	X
All changes to the Token profile	X
Changes to an EAG Federation profile	-
Appointment of an individual to a Trusted Role	X
Designation of personnel for multiparty control	X
Installation of the Operating System	X
Installation of the Application	X
Installation of hardware cryptographic modules	X
Removal of hardware cryptographic modules	X
Destruction of cryptographic modules	X
System Startup	X
Logon attempts to the Application	X
Receipt of hardware / software	X
Attempts to set passwords	X
Attempts to modify passwords	X
Back up of the internal OTP database	X

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

Auditable Event	OTPS
Restoration from back up of the internal OTP database	X
File manipulation (e.g., creation, renaming, moving)	X
Posting of any material to a Repository	X
Access to the internal OTP database	X
All Token compromise notification requests	X
Loading tokens with Tokens	X
Shipment of Tokens	X
Activation of Tokens	X
Deactivation of Tokens	X
Token Re-Sync	X
Successful and unsuccessful remote proofing, proofer-based proofing, and user registration	X
Cancellation or failure of remote proofing, proofer-based proofing, and user registration	X
Successful and failed knowledge-based pin and proofing	X
Successful mail-based proofing	X
Successful and failed proofer-based proofing	X
Successful and unsuccessful use of mail-based and proofer-based activation codes	X
Successful activation of an SMS/IVR/APP-based authentication device	X
Failure to activate an SMS/IVR/APP-based authentication device	X
Removal of an SMS/IVR/APP-based authentication device from user's account	X
Suspension or re-enablement of an SMS/IVR/APP-based authentication device on a user's account	X
Changes to Hardware	X
Changes to Software	X
Changes to Operating System	X
Patches	X
Changes to Security Profiles	X
Personnel Access to room housing Component	X
Access to the Component	X
Known or suspected violations of physical security	X
Software error conditions	X
Software check integrity failures	X

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

Auditable Event	OTPS
Receipt of improper messages	X
Misrouted messages	X
Network attacks (suspected or confirmed)	X
Equipment failure	X
Electrical power outages	X
Uninterruptible Power Supply (UPS) failure	X
Obvious and significant network service or access failures	X
Violations of Token Policy	X
Violations of Certification Practice Statement	X
Resetting Operating System clock	X

5.4.2 Frequency of Processing Audit Logs

Audit logs shall be reviewed at least once every 30 days. Statistically significant sample of security audit data generated by the OTPS since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. The Audit Administrator shall explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained onsite for at least sixty days as well as being retained in the manner described below. For the OTPS, Audit Administrator shall be the only person responsible to manage the audit log (e.g., review, backup, rotate, delete, etc.).

5.4.4 Protection of Audit Logs

System configuration and procedures shall be implemented together to ensure that:

- Only authorized people have read access to the logs;
- Only authorized people may archive audit logs; and,
- Audit logs are not modified.

The person performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access). Audit logs shall be moved to a safe, secure storage location separate from the OTPS equipment.

It is acceptable for the system to over-write audit logs after they have been backed up and archived.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least once every 30 days. A copy of the audit log shall be sent to a secure off-site storage location every 30 days.

5.4.6 Audit Collection System (internal vs. external)

The audit log collection system may or may not be external to the OTPS. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the Exostar OA shall determine whether to suspend operation until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

This OP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

Exostar shall perform perimeter network vulnerability assessments no less frequently than on a monthly basis.

Static and dynamic web application scanning shall be conducted on a periodic basis for critical authentication and assertion functions.

EPCS members may elect to perform additional security assessments (e.g. network, application, operational security, Red Team scenarios) with prior notice and coordination with the Exostar PMA, Security Program, and Security Office.

In the event that a vulnerability is identified in the OTP authentication device and the OTP authenticator is no longer acceptable, Exostar will remediate the vulnerability to an acceptable risk level and consider replacing the device if necessary

5.4.9 Types of Records Archived

MAG, EAG, and OTP archive records shall be sufficiently detailed to establish the proper operation of the component or the validity of any Token (including those revoked or expired) issued by the OTPS.

Data To Be Archived	OTPS
One Time Password Practice Statement (OPS)	X
Contractual obligations	X
System and equipment configuration	X
Modifications and updates to system or configuration	X
Token requests	X
Revocation requests	X
Subscriber identity authentication data as per Section 3.2.3	X
Documentation of receipt and acceptance of Tokens	X

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

Data To Be Archived	OTPS
Documentation of receipt of Tokens	X
All Tokens issued or published	X
Record of Component Token Re-Sync	X
All Audit Logs	X
Other data or applications to verify archive contents	X
Documentation required by compliance auditors	X

5.4.10 Retention Period for Archive

The minimum retention periods for archive data is 7.5 years for Exostar OTPS proofing, provisioning, re-sync, and de-provisioning events.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Alternatively, Exostar may retain data using whatever procedures have been approved by NARA for that category of documents. Applications required to process the archive data shall also be maintained for the minimum retention period specified above.

5.4.11 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the OTPS, the authorized individuals are Audit Administrators. The contents of the archive shall not be released except as determined by the Exostar PMA or as required by law. Records of individual transactions may be released upon request of any Subscriber involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the Exostar MAG, EAG, SAM, or OTP production servers with physical and procedural security controls equivalent to those for component.

5.4.12 Archive Backup Procedures

The OPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.4.13 Requirements for Time-Stamping of Records

OTPS archive records shall be automatically time-stamped as they are created. The OPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.4.14 Archive Collection System (internal or external)

Archive records shall be transferred and stored to a trusted system that is managed by Audit Administrator personnel independent of the Exostar OA.

5.4.15 Procedures to Obtain & Verify Archive Information

Procedures detailing how to create, verify, package, and transmit archive information shall be defined in the OPS.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

5.5 Key Changeover

The following table provides the life times for the private keys used in the OTPS. To minimize risk from compromise of the OTPS private encryption keys, the keys may be changed more frequently.

Key	Symmetric Key Algorithm	
	3DES	AES-128 or 256
Production Token Transit Key	(Changed with Each Token Batch)	(Changed with Each Token Batch)
ORDB Encryption Key	10 years	10 years

5.6 Compromise and Disaster Recovery**5.6.1 Incident and Compromise Handling Procedures**

If the Exostar OA detects a potential hacking attempt or other form of compromise, it shall perform an investigation in order to determine the nature and the degree of damage. If the OTPS keys or identity data are suspected of compromise, a major security incident (“Security Incident” or “Security Breach”) shall be declared by Exostar management, the incident response procedures outlined in Section 5.6.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the OTPS needs to be rebuilt, only some Tokens need to be revoked, and/or the OTPS needs to be declared compromised.

The Exostar PMA, Security Program, and Security Office shall be notified by the Exostar OA if any of the following cases occur:

- suspected or detected compromise of the OTPS system;
- physical or electronic attempts to penetrate the OTPS system;
- denial of service attacks on the OTPS component; or
- OTPS is inoperable.

The ESPC shall be notified in a timely manner if any of the following cases occur:

- MAG, SAM, EAG, BAID, or OTP are inoperable beyond their uptime SLA; or
- any incident materially impacting the integrity or confidentiality of OTP or identity data is identified.

The above measures will allow Relying Parties to protect their interests, as may be appropriate to the specific circumstances.

The Exostar OA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the respective OPS.

5.6.2 Computing Resources, Software, and/or Data are Corrupted

If OTPS equipment is damaged or rendered inoperative, but the OTPS encryption keys and identity data are not destroyed, operation shall be re-established as quickly as possible, giving priority to the ability to authenticate Subscribers.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

5.6.3 Private Key and OTPS Compromise Procedures

In the event that Exostar discovers or is notified of a Security Incident or Security Breach affecting Relying Party systems or information, Exostar shall immediately;

- a) establish a confidential communications channel and notify designated Relying Party security points of contact of key incident details;
- b) if Relying Party information was in the possession of Exostar at the time and location of the Security Incident or Breach, and is reasonably believed to have been affected, Exostar shall (i) investigate and use best efforts to cure the actual Security Breach; (ii) assist affected Relying Parties in investigating, remedying, and taking other practical actions deemed necessary to address the incident and any dispute, inquiry, or claim that relates to the Security Incident, as mutually agreed by Exostar and the Relying Party; (iii) except with respect to Security Breaches that originated with or were caused by a Relying Party or Subscriber Organization, provide assurance satisfactory to the Relying Party that the Security Breach will not recur.

If ORDB encryption or Subscriber token keys are compromised or suspected to be compromised:

1. All Relying Parties shall be securely notified at the earliest feasible time, so that partners may take appropriate action;
2. If Subscriber data integrity is found to be intact, but OTPS binding data is not, Relying Parties may revert to single-factor authentication (password).

The Exostar PMA and Security Office shall investigate what caused the compromise or loss, and what measures must be taken to preclude recurrence.

5.6.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby the Exostar MAG, EAG, SAM, BAID, or OTP service is physically damaged and cannot be recovered at the primary production facility within a pre-determined period of time, the Exostar PMA shall invoke Exostar's Business Continuity Plan and applicable disaster recovery plans at its alternate processing site.

The Repositories containing MAG, EAG, SAM, BAID, and OTP information shall be deployed so as to provide 24 hour per day/365 day per year availability. Exostar shall implement features to provide high levels of authentication service and repository reliability targeting (99.9% availability or better).

5.7 OTPS Termination**5.7.1 Subscriber Termination**

In the event of termination of an OTP Subscriber's use of the OTPS, Exostar shall revoke all OTP hardware, SMS, IVR, or APP tokens issued to the Subscriber. Upon termination of the service, Exostar will maintain user data under the same controls as described in section 5.4.10.

5.7.2 Organization Termination

In the event of termination of an OTP Subscriber Organization's service agreement, Exostar shall revoke all OTP hardware, SMS, IVR, or APP tokens issued to the Subscriber Organization. Upon

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

termination of the service, Exostar will maintain user data under the same controls as described in section 5.4.10.

5.7.3 Service Termination

In the event of OTP Service termination, Exostar shall provide notice to all Relying Party Subscriber Organizations prior to the termination, providing as much advance notice as circumstances permit.

Upon termination of the service, Exostar will maintain user data under the same controls as exist when the service is active, or will destroy the data as permitted. The Exostar OA shall archive all OTPS audit logs and other records, and shall destroy all OTPS keys upon termination.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The following table provides the requirements for key generation.

Entity	FIPS 140-1/2 Level	Hardware or Software	Same Module
ORDB Encryption	2 or higher	Hardware	Same

Random numbers forming the basis for hardware OTP token secrets shall be generated in FIPS 140 Level 2 validated hardware cryptographic modules.

Random numbers forming the basis for SMS-, IVR-, or APP-delivered OTP secrets may be generated using software-based pseudo-random number generators. FIPS 140 validated modules are recommended, but are not required for generation of SMS-, IVR-, and APP-delivered secrets, or for associated Proofer signature or postal mail delivery processes.

OTPS key pair generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. The process shall be validated by an independent third party.

6.1.2 Private Key Delivery to Subscriber

Not applicable to the OTPS.

6.1.3 Public Key Delivery to Token Issuer

Not applicable to the OTPS.

6.1.4 OTPS and Transport Key Delivery to Relying Parties

The HOTP transport key shall be provided to the Exostar OA via an auditable and trusted process.

Acceptable methods for delivery include but are not limited to:

- In-person transfer of media between trusted personnel; or
- Secure distribution through secure out-of-band mechanisms (double-wrapped mail or package transport, with signature required on delivery).

6.1.5 Key Sizes

All OTPS cryptographic components and Transport Layer Security (TLS) protocols shall use the following algorithm suites.

Cryptographic Function	Specification
Signature	Minimum of 2048 bit RSA per FIPS 186-3
Hashing	SHA-1 (Deprecated, but permitted on an exception basis to meet third party hardware/software constraints), or SHA-256
Public Key Encryption	Minimum of 2048 bit RSA
Symmetric Encryption	AES / 3 Key TDES

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*. Cryptographic modules shall be validated to the FIPS 140-2 level identified in section 4.19.1.

6.2.2 Private Key Multi-Person Control

Use of the ORDB encryption key shall require two Trusted Role personnel, procedurally enforced.

6.2.3 Private Key Escrow

Under no circumstances shall the ORDB encryption key be escrowed by a third party.

6.2.4 Private Key Backup

6.2.4.1 Backup of ORDB Private Encryption Key

The ORDB private encryption keys shall be backed up under the same multi-person control as the original encryption key. A single backup copy of the encryption key shall be stored at or near the OTPS location. A second backup copy shall be kept at the OTPS backup location. Procedures for OTPS private encryption key backup and restoration shall be included in the appropriate OPS and shall meet the multiparty control requirement of Section 5.2.2.

6.2.5 Private Key Archival

Private encryption keys shall not be archived by the OTPS.

6.2.6 Private Key Transfer into or from a Cryptographic Module

ORDB encryption keys shall be generated by and remain secured by a cryptographic module. ORDB encryption keys shall not be exported.

Transfer and backup of ORDB keys shall be conducted in a secure manner between hardware storage modules.

6.2.7 Private Key Storage on Cryptographic Module

The cryptographic module may store private and symmetric keys in any form as long as the keys are not accessible without authentication mechanism that is in compliance with FIPS 140-2 rating of the cryptographic module.

6.2.8 Method of Activating HSM-Controlled Keys

The OTP runtime application will utilize a cryptographic module which does not require operator intervention for module activation.

Practice Note: A Thales/nCipher HSM module-protected key with passphrase-protected Administrator Card Set (ACS) smart cards and no Operator Card Set (OCS) or runtime passphrase activation satisfies this requirement.

The OTP token manufacturer may utilize a cryptographic module with or without activation data. If utilized, acceptable means of authentication include but are not limited to pass-phrases, PINs or

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Methods of Deactivating HSM-Controlled Keys

Cryptographic modules that have been activated shall not be left available to unauthorized access. Hardware cryptographic modules shall be removed and stored in a secure container when not in use by the OTPS production applications.

6.2.10 Method of Destroying HSM-Controlled Keys

ORDB private encryption keys shall be destroyed when they are no longer needed, or when all tokens to which they correspond expire or are revoked. For hardware cryptographic modules, this will likely be executing a “zeroize” command. Physical destruction of hardware should not be required.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Activation Data

6.3.1 Activation Data Generation and Installation

The activation data used to unlock private and symmetric keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the security policy requirements of the cryptomodule used to store the keys. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.3.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data for HSM administrator card sets shall not be entered from remote workstations, unless dedicated hardware and Specialized Security Limited Functionality (SSLF) profile is utilized. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

6.3.3 Other Aspects of Activation Data

The Exostar OA shall change the activation data whenever the HSM is re-keyed or returned from maintenance.

6.4 Computer Security Controls

6.4.1 Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The OTPS shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

- Provide a security audit capability
- Prohibit object re-use
- Require use of cryptography for session communication and database security
- Require a trusted path for identification and authentication
- Provide domain isolation for process
- Provide self-protection for the operating system
- Require self-test security related OTPS services (e.g., check the integrity of the audit logs)
- Support recovery from key or system failure

When OTPS equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

The computer system shall be configured with a minimum of required accounts, network services, and controls to limit and audit remote login to only authorized remote administrative systems (e.g. bastion hosts and designated Exostar OA workstations).

An administrative 'superuser' credential shall be established for all production OTPS components under multi-party Trusted Role control and shall be retained in an emergency escrow location and controlled as described in Exostar OA procedures.

6.4.2 Computer Security Rating

The OTPS shall utilize Common Criteria and other server hardening configurations such as the CIS baseline, as described in the OPS.

6.5 Life-Cycle Technical Controls

6.5.1 System Development Controls

The System Development Controls for the OTPS are as follows:

- Use software that has been designed and developed under a formal, documented secure development methodology.
- Hardware and software procured shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Hardware and software developed shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- Production server hardware, virtualization components, operating systems, and software shall be dedicated to performing OTP and IdM-related activities. There shall be no other applications, hardware devices, network connections, or component software installed which are not part of MAG, EAG, SAM, BAID, ProviderPass, OTPS, and related service operation. However nothing in this clause shall prohibit production OTP and IdM server hardware from residing within a larger/converged enclosure (e.g. blade enclosure) that may also house non-TR server hardware providing non-OTP and non-IdP related services, and sharing essential modules with those servers (e.g. power, network), so long as a) the servers or clusters of servers providing OTP and IdM-related activities are dedicated to those activities, b) the backplane of said enclosure does not introduce additional attack vectors, or those vectors are mitigated with compensating controls, and c) the entire enclosure is physically protected as described in section 5.1.
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform operations shall be allowed and obtained from sources authorized by local policy. OTPS hardware and software shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.
- Patch and vulnerability management shall be conducted in accordance with the Exostar Information Security Policy, established detection and remediation timelines, and industry best practices.

6.5.2 Security Management Controls

The OTPS production service shall be deployed in a secure server/network environment, which is separate from Exostar's test, development, and corporate back-office networks.

A tiered production server architecture shall be established to segregate web/proxy tier, application tier, database and data repository, and administrative server interfaces. Communication between server tiers shall be conducted via Stateful-Packet Inspection (SPI) firewalls.

Communication across server and network tiers shall be monitored by network-based intrusion detection systems (NIDS). Network flow traffic (e.g. Netflow or JFlow) and full packet capture shall be utilized where feasible, and to the extent that OTPS confidentiality is not affected.

Interoperation of networks shall be limited to defined server and application interfaces.

Local administration of OTPS servers shall be conducted via direct console (e.g. KVM) connections.

Remote administration of OTPS servers shall be conducted using bastion hosts which are part of the production Trusted Role server environment and shall include use of host IDS feeds to a Security Information and Event Management (SIEM) database.

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

Access to the bastion hosts described above for remote administration of OTPS servers shall be limited to dedicated hardware or virtual workstations (i.e. direct access to the bastion hosts shall not be possible from general issuance-laptops or PCs) in support of APT defense and shall include use of host IDS feeds to a Security Information and Event Management (SIEM) database. Where dedicated virtual workstations are used, these virtual workstations shall be isolated on a dedicated VLAN available only to TR Administrators, accessible only from an Exostar corporate general-issuance laptop or PC which has been specially configured for TR Administrators to access the dedicated VLAN within the corporate Exostar network infrastructure. This VLAN shall have no access to the Internet. The dedicated virtual workstation shall be accessible only via an encrypted and authenticated protocol (e.g. PCoIP), and the client used to access this workstation shall be digitally signed by the vendor with a code-signing certificate issued by a trusted CA.

Remote administration of OTPS server components, including the controlled OTP Administration (OAdm) interface, shall utilize multi-factor authentication methods which are at least as strong as the OTPS credentials being managed. Where remote administration is conducted using the virtual workstation described above, access to both the virtual workstation host and the server bastion host shall require shall utilize separate and distinct multi-factor authentication methods which are at least as strong as the OTPS credentials being managed.

6.5.3 Life Cycle Security Controls

The OTPS shall be managed under change management controls defined in the OPS.

A production-representative test environment shall be established and maintained in support of the production OTPS environment.

A production change control board shall track, approve, and schedule all system and configuration changes in the OTPS production and test environments.

6.6 Network Security Controls

The Exostar OTPS shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of Exostar-dedicated firewalls, switches, and filtering routers which are managed under the Exostar OA. Unused network ports and services shall be disabled or removed. Any network software present shall be necessary to the function of the OTPS and IdM services.

Any boundary control devices used to protect the network on which OTPS equipment is hosted shall deny all but the necessary services to the equipment even if those services are enabled for other devices on the network.

In addition to the audit and archival controls specified in Section 5.4 and 5.5, operational security event logging, aggregation, and correlation rules shall be utilized to detect potential security incidents within the OTPS and on controlled production and administrative network segments.

Technologies including Security information and event management (SIEM), Netflow, network full packet capture, and server memory state forensics shall be permitted provided that such supporting technologies are managed as part of the controlled Exostar Trusted Role environment.

Third party security monitoring, operational and incident response services may be utilized if appropriate security controls and flow-downs are applied in contracts between Exostar and the third party provider.

6.7 Time Synchronization and Time Stamping

OTPS server components shall utilize an Exostar-standardized time synchronization service (e.g. dedicated NTP server) which in turn synchronizes with a trusted Internet time source.

6.8 High Availability Architecture

To meet SLA goals, the OTPS may be deployed in a High Availability (HA) configuration between multiple production sites/datacenters in a geographic region; however, all Facility Management & Operational Controls (Section 5), and Technical Security Controls (Section 6) shall be met by all production sites in their entirety, with specific attention given to the additional off-site backup requirements for this architecture documented in Section 5.1.8.

Any OTPS data, specifically including but not limited to ORDB data, machine images, virtualization and network settings, etc. replicated between HA sites shall only be transmitted over a dedicated Layer 1 or Layer 2 circuit (e.g. MPLS, Metropolitan Area Ethernet, etc.) and encrypted at the circuit, network, protocol, file, or application layer using only the approved key sizes and algorithms defined in Section 6.1.5.

security

7 [RESERVED]

8 COMPLIANCE ASSESSMENTS

The Exostar OTPS shall have a compliance assessment mechanism in place to ensure that the requirements of the OP/OPS are being implemented and enforced.

8.1 Frequency or Circumstances of Assessments

The Exostar OTPS shall be subject to periodic internal compliance assessments, at least once every 30 days. The Exostar OTPS may be subject to an external compliance assessment as needed to maintain third party certifications and accreditations, as directed by the Exostar PMA and Security Program.

8.2 Identity and Qualifications of Assessor

The Exostar Audit Administrators shall conduct internal compliance assessments.

An external compliance assessor may be designated by the Exostar PMA and Security Program. The assessor shall demonstrate competence in the field of compliance audits, and shall be thoroughly familiar with requirements of this OP.

8.3 Assessor's Relationship to Assessed Entity

The compliance assessors shall be independent from the Exostar OA. The Exostar PMA, Security Program, and Security Office shall determine whether a compliance auditor meets this requirement.

8.4 Topics Covered by Assessment

The purpose of a compliance assessment shall be to verify that the OTPS operates in accordance with this OP, the OPS, and the applicable MOAs between Exostar and other Relying Parties.

8.5 Actions Taken as a Result of Deficiency

The Exostar PMA, Security Program, and Security Office may determine that the OTPS or an integrated Service Provider application is not complying with its obligations set forth in this OP. When such a determination is made, the Exostar PMA may temporarily suspend operation of the OTPS or integration with a noncompliant Service Provider application, or may direct the Exostar Operational Authority to apply corrective actions to allow interoperation to continue.

If the compliance assessor finds a discrepancy between how the OTPS is designed or is being operated or maintained, and the requirements of this OP or the applicable OPS, the following actions shall be performed:

- The compliance assessor shall note the discrepancy;
- The compliance assessor shall notify the Exostar PMA and Security Program of the discrepancy;
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this OP, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Exostar PMA may decide to temporarily halt operation of an Exostar OTPS, to revoke a Token

Exostar One-Time Password (OTP) Policy v2.4 – Exostar Confidential

issued by the Exostar OTP service, or take other actions it deems appropriate. The Exostar PMA shall develop procedures for making and implementing such determinations.

8.6 Communication of Results

A periodic compliance assessment report, including identification of corrective measures taken or being taken, shall be provided to the Exostar PMA as set forth in Section 8.1. The report shall identify the versions of the OP and OPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in 8.5 above.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Use and Governing Agreements

Use of the Exostar Managed Access Gateway (MAG), Enterprise Access Gateway (EAG), Secure Access Manager (SAM), ProviderPass, and One Time Password (OTP) services is governed by applicable laws, regulations, and Subscriber Organization service agreements, including the Exostar Privacy Policy and Exostar General Terms and Conditions.

10 ACRONYMS & ABBREVIATIONS

APP	Mobile Device Authenticator Provider
BAID	Boeing Aviation ID
FDCC	Federal Desktop Core Configuration
HA	High Availability
HMAC	Hash-based Message Authentication Code
HOTP	HMAC-based One Time Password algorithm (see IETF RFC 4226)
IETF	Internet Engineering Task Force (www.ietf.org)
MAG	Managed Access Gateway
OATH	Initiative for Open Authentication (www.openauthentication.org)
OP	One Time Password Policy
OPS	One Time Password Practices Statement
OTP	One Time Password
OTPS/SOTP	One Time Password System / Shared One Time Password
PMA	Policy Management Authority
PKI	Public Key Infrastructure
RFC	Request for Comments
SAM	Secure Access Manager
SSLF	Specialized Security – Limited Functionality

Certificate Of Completion

Envelope Id: E83D967BA1064BB6B98E391BBBC172DF	Status: Completed
Subject: Complete with DocuSign: Exostar OTP Policy v 2 4 .pdf	
Source Envelope:	
Document Pages: 58	Signatures: 1
Certificate Pages: 2	Initials: 0
AutoNav: Enabled	Envelope Originator:
Enveloped Stamping: Enabled	Michelle Underwood
Time Zone: (UTC-05:00) Eastern Time (US & Canada)	2325 Dulles Corner Blvd
	Suite 600
	Herndon, VA 20171
	michelle.underwood@exostar.com
	IP Address: 148.59.73.122

Record Tracking

Status: Original	Holder: Michelle Underwood	Location: DocuSign
2/16/2023 12:31:54 PM	michelle.underwood@exostar.com	

Signer Events

Ming Chan
Ming.Chan@exostar.com
Manager, Governance & Engineering
Exostar, LLC
Security Level: Email, Account Authentication (None)

Signature

DocuSigned by:

6F4BB9D4FF3047F...
Signature Adoption: Pre-selected Style
Using IP Address: 136.226.48.202

Timestamp

Sent: 2/16/2023 12:55:26 PM
Viewed: 2/16/2023 2:11:00 PM
Signed: 2/16/2023 2:11:28 PM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events

Signature

Timestamp

Editor Delivery Events

Status

Timestamp

Agent Delivery Events

Status

Timestamp

Intermediary Delivery Events

Status

Timestamp

Certified Delivery Events

Status

Timestamp

Carbon Copy Events

Status

Timestamp

Theresa Fleming
Theresa.Fleming@exostar.com
Security Engineer
Security Level: Email, Account Authentication (None)

COPIED

Sent: 2/16/2023 12:55:25 PM
Viewed: 2/16/2023 1:48:15 PM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Witness Events

Signature

Timestamp

Notary Events

Signature

Timestamp

Envelope Summary Events

Status

Timestamps

Envelope Sent	Hashed/Encrypted	2/16/2023 12:55:25 PM
Envelope Updated	Security Checked	2/16/2023 1:00:44 PM
Certified Delivered	Security Checked	2/16/2023 2:11:00 PM
Signing Complete	Security Checked	2/16/2023 2:11:28 PM
Completed	Security Checked	2/16/2023 2:11:28 PM

Payment Events

Status

Timestamps