Product Overview

Exostar’s Federated Identity Service (FIS) is a fully-managed public key infrastructure (PKI) service for the issuance and maintenance of digital certificates. As part of a suite of identity management services offered by Exostar, FIS is a comprehensive PKI solution that enables full lifecycle management of certificates, strong authentication practices, and controlled access to applications through Exostar Managed Gateway minimizing risk and assuring resources and intellectual assets are protected over the extended enterprise. Because FIS adheres to the requirements of industry PKI bridge partner such as SAFE BioPharma, as well as Federal best-practice guidelines, it is ideal to enable sensitive online transactions and secure access to information.

Exostar’s Managed PKI Solution

Exostar hosts, manages and maintains the entire PKI certification process and the servers that provide the Web-based registration interface for administrators and users. In addition, Exostar plays a key role in the design and framework of secure, collaborative solutions in order to promote continued interoperability for large-scale industry and industry-to-government programs.

BENEFITS

- Lowers costs by consolidating redundant operations and optimizing existing technical infrastructure/resources
- Accelerates deployments with open, standards-based protocols and certificate policies that enable identities/entitlements to be shared across systems/domains
- Enhances productivity by alleviating in-house resources of the burden of building, operating and maintaining complex PKI infrastructure
- Assures identity validity via integrated, multi-layered security and authentication practices
- Meets critical technical, regulatory requirements
- Encourages rapid adoption of PKI-enabled services by partners, customers, suppliers through seamless interoperability with Intranets, Extranets, VPNs

EXOSTAR VALUE

Exostar recognizes that identity management goes beyond the traditional issuance of PKI - it’s about delivering secure and controlled access to networks and applications inside and outside the organization. Exostar’s unmatched expertise in highly secure environments, industry to government experience and proven worldwide solutions deliver on the vision:

Exostar FIS certificates are trusted by the Federal Bridge Certificate Authority, and the Dept. of Defense
Exostar has been approved as a Full Service Credential Service Provider (CSP) by the SAFE-BioPharma Trust Framework.
FIS provides credentials Medium level of assurance (MLOA) credentials software
Operates on-demand, secure networks for some of the largest organizations in Aerospace & Defense, Life Sciences and the Financial markets with over 100,000 companies worldwide
Capabilities

Certificate Authority
Certificates comply with ISO, IETF, US Federal, A&D PKI standards
Protected repository of private encryption keys with retention and access processes based on policy
Certificate Revocation Lists published every 12 hours
Real-time validation of certificates for administrators through OCSP
Support for client authentication, digital signature, encryption certificates; 3rd party credentials may be supported with Federation

Federal Bridge Certification Authority (FBCA)
Interoperability certification for PKI services based on the latest National Institute of Standards and Technology (NIST) SHA-2 standard.
Medium software, hardware assurance level means PKI services, operations, infrastructure performed with moderate risk of data compromise
Cross-certification with U.S. Federal Bridge enables interoperability between industry and federal government

Registration Authority
Web-based interface for end users for certificate enrollment, renewal, modification, with auto-reminders for lifecycle events
Lifecycle certificate management/process tool for administrators
Support for in-person identity-proofing ceremony per Federal Bridge
Registration repository maintained for 10.5 years

Security Management
Military-grade hosting facilities include fortified construction, multi-layered security system, dual biometric access control, 24-hour monitoring, inside/outside camera surveillance, high-density power systems
Role-based access control
Investigative background checks, and training for trusted personnel
Annual physical & logical audits by third-party auditors
Key changeover/re-key process, with new keys every 3 years
CA root keys network-isolated, stored in secure, off-site location

Infrastructure Operations
Guaranteed 24/7 uptime support/availability (excluding planned downtimes)
End-to-end system redundancy
Backup disaster recovery “hot” sites that operate 24/7

Customer Service
Live telephone support (3 AM – 11 PM ET)
24/7 off-hours paging service for Severity 1 priorities
Online training and documentation

TECHNICAL REQUIREMENTS

X.509 v3 certificate standard
Client authentication certificates
Digital signature certificates
Encryption certificates
2048 RSA key size
SHA-2 Support
LDAP or HTTP protocols for repository and OCSP access

SYSTEM REQUIREMENTS

Microsoft Windows Vista or later operating systems
Microsoft Internet Explorer 7.0 or later Internet browsers
Keys installed on workstations for Medium Soft key issuance (optional)
FIPS 140 level 2 or higher smart cards for Medium Hard assurance for Smartcards or Smart Tokens (optional)

Exostar, LLC.
13241 Woodland Park Road
Suite 400
Herndon, VA 20171
USA
Phone: 1-703-793-7800
Fax: 1-703-793-7962
www.exostar.com