



## PROTEXX PKI-VPN ENCRYPTION

### Consumer Encryption

#### Key Features and Benefits

- Anonymizer safeguards your IP from theft
- Remote VPN protects against hacking and identity theft
- Secures Your Wi-Fi Hotspot Connections
- Secures Your Network Connections
- Secures Your Home, Office, Cable and High Speed DSL Access
- Secures Your email and File Transfers
- Safe and Encrypted Connections Between Your Computer and the Internet

### Enterprise Encryption

#### Key Features and Benefits

- You receive all of the Consumer benefits *plus*
- Standards-based Security
- RSA trusted root certificates
- Simple corporate-wide deployment
- Identity Management Administrative controls
- Remote VPN capabilities
- Ability to instantly allow secure external links for remote employees
- Capability for secure access for contractors and customers

### Government Encryption

#### Key Features and Benefits

- Offered exclusively through ECA.ORG.com
- GSA ACES Program
- Identification/Digital Signature
- Government Trusted ECA
- Server Authentication for identification of web sites and other devices
- Domain Controllers for securing your Windows domain
- Signing of Code
- HSPD-12 Compliant
- FIPS-201 Compliant
- Full auditing and compliance

# Protexx Managed Public Key Infrastructure (PKI)

The Protexx® Managed Public Key Infrastructure (PKI) service is a fully integrated enterprise solution designed to secure intranet, extranet, and Internet applications while enabling fluid interaction with business partners, mobile workers, Web services devices, and other users. This highly scalable service allows enterprises to rapidly establish a robust PKI and certificate authority (CA) system while alleviating the burden of PKI deployment, maintenance, and oversight. Enterprises retain complete control over security policy, authentication models, and certificate lifecycle management. Built on open standards to ensure maximum flexibility, the Protexx Managed PKI service allows interoperability with virtually any application or device. By leveraging the Managed PKI service to deploy digital certificate services, enterprises can reduce the cost and complexity of PKI implementations while providing globally trusted, state-of-the-art authentication, encryption, digital signing, and non-repudiation services within and beyond the enterprise.

## + Fast, Scalable Implementation

Easy-to-use toolkits and pre-integration with leading applications and platforms ensures rapid deployment of the Protexx Managed PKI service on virtually any system, network, or device, whether located within the enterprise or externally. The Managed PKI service has been proven under real-world conditions to scale smoothly from thousands to hundreds of thousands of users, allowing enterprises to deploy digital certificates on an as-needed basis. In addition, because all services are hosted on Protexx's existing infrastructure, implementation can be completed in a matter of weeks.

## + Secure, User-Friendly Remote Access

The Protexx Managed PKI service provides the ability to transparently use digital certificates for strong authentication in wired and wireless access environments. Roaming capabilities enable mobile end users, working from any Internet-enabled PC or device, to seamlessly use digital certificates when accessing intranets, extranets, Web applications, and Web portals. Depending on business requirements, enterprises can choose an entry-level, single-server model roaming service or a more robust, multi-server model service. Finally, integration with smart cards, biometric drives, USB tokens, and Trusted Platform Modules on Intel® Centrino™, Apple Mac and Linux based platforms, enables the use of a variety of two-factor and three-factor authentication solutions for remote access.

## + Long-Range Flexibility

Protexx is committed to open standards, innovative technology, and strategic collaborations, to promote the flexibility and ease of use that enterprises need to not only operate freely in diverse environments, but also to maximize return on existing investments. The Protexx Managed PKI service supports standard X.509v3 certificates with delivery by PKCS12. Managed PKI operates on current versions of popular browsers such as Internet Explorer, Mozilla Firefox® and a variety of operating systems, including Windows, Solaris,™ and AIX.® in the Protexx® Certificate Access Portal (CAP) enables enterprises to present a common, brand-able user interface for digital certificate services, even in heterogeneous subscriber platform environments.

## + Industry Compliance

The Protexx/Widepoint Managed PKI service is the first managed PKI to achieve Federal Bridge Certification Authority compliance, allowing enterprises to interoperate easily with federal agency PKIs. In addition, the Protexx Managed PKI service helps enterprises comply with industry-specific government mandates regarding the protection, availability, and audit-ability of sensitive data. Using Managed PKI services, healthcare services providers, financial institutions, government agencies, insurance companies, and other organizations

can authenticate, encrypt, sign, and audit data exchanges to support compliance with federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), California Senate Bill 1386, the Gramm-Leach-Bliley Act, and 21 CFR Part 11.

### **+ PKI Modernization Program**

In response to the growing trend of companies moving away from proprietary PKI software systems, Protexx is offering a program to enable enterprises and government agencies using proprietary PKI vendor software to quickly, easily, and cost-effectively migrate to next-generation Protexx Managed PKI services. Special pricing incentives and technical assistance is available for customers looking to upgrade from proprietary software to next-generation PKI service solutions.

## **Protexx PKI-VPN Product Features**

- \* Significant cost savings compared to traditional strong authentication solutions
- \* No hardware tokens to issue, repair or replace
- \* Client side software required for the end user
- \* A wide range of authentication modalities that can be custom configured
- \* An option for conducting an implementation that is completely transparent to the end user
- \* IP analytics comparison of network information collected during previous login attempts
- \* Location-based authentication via IP based geo-location technology
- \* Protection against a wide range of online fraud threats including man-in-the-middle attacks
- \* Asymmetrical Authentication deployed capability that protects against phishing attacks and allows for both site-to-user and user-to-site verification
- \* Flexible and easy-to-configure administration management platform

## **Authentication**

X509 Certificate Authentication  
MXI Stealth Biometrics  
CAC Card Access

## **Threat Assessment**

Real-time Online Fraud Management integration module

## **Regulatory and Standards Compliance**

OpenSSL has a FIPS 140-2 certification  
OpenVPN approved for HLS use

## **Managed Identity Services Qualifications**

Authorized by the US Government to issue credentials applying strong authentication since 1999, a division of our parent company ORC is a designated Shared Service Provider with operational experience in all facets of identity assurance.

- Fully compliant ECA and ACES certificates via website or walk-in application
- 1st Certified & Accredited HSPD-12 Compliant GSA Shared Service Provider - GSA SIN 132-61
- Federal Bridge Certificate Authority (FBCA) Cross-Certified
- A Certified & Accredited GSA Access Certificates for Electronic Services (ACES) - GSA SIN 132-60
- PIVotal ID™ certificate solutions that comply with HSPD-12 requirements

- Pre-engineered solutions that save the cost of R&D, yet custom-fit to your organization
- Managed validation services to monitor multiple Certificate Authorities for faster feedback
- Managed translation services that allow access to multiple user sites with a single password
- Assurance Level 1, 2, 3 and 4 credentials
- A Certified & Accredited GSA HSPD-12 End-to-End Managed Service Provider - GSA SIN 132-62
- 1st Certified & Accredited commercial GSA E-Authentication Service Provider