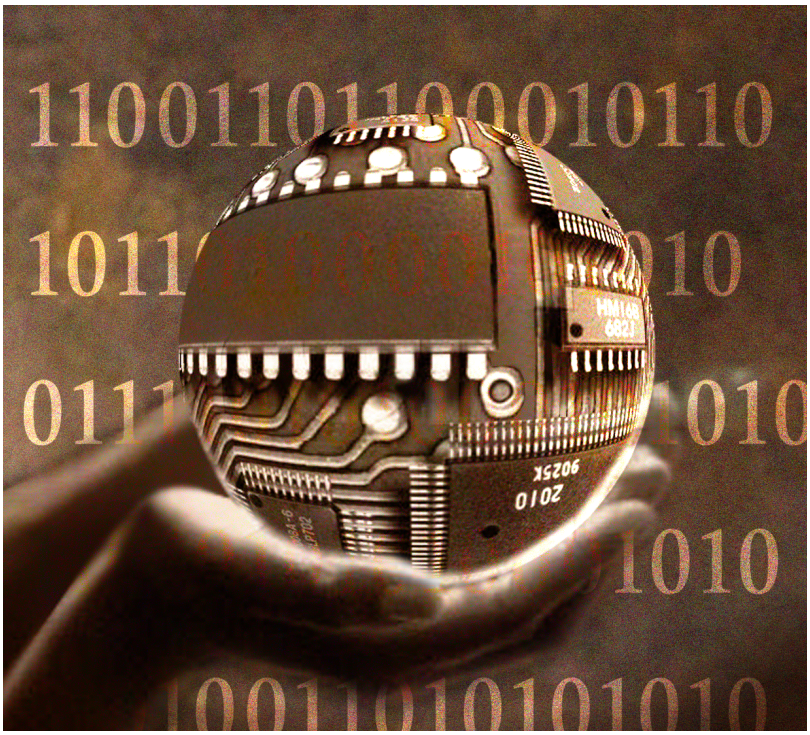
msctrustgate.com

Managed PKI

The Integrated Public Key Infrastructure Platform



The **Managed Public Key Infrastructure** (MPKI) 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. The highly scalable service allows enterprises to rapidly establish a robust PKI and certificate authority (CA) system with complete control over security policy, authentication models, and certificate lifecycle management.

Built on open standards to ensure maximum flexibility, the Managed PKI service allows interoperability with virtually any application or device, and is pre-integrated with leading off-the-shelf solutions, including Microsoft applications and Windows operating systems. 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.

The suite of Managed PKI services includes:

Go Secure! Solutions
This suite of managed applications services has been created especially to help your enterprise secure its most vital transaction and communication applications. Incorporate digital certificate-based authentication into your existing e-mail applications, VPN devices, Web applications and ERP solutions.

Roaming
The Roaming Service technology enables enterprises and consumers to securely download private data and digitally sign transactions, using digital certificates as credentials, from virtually any Internet-enabled PC or mobile devices.

Key Benefits

- **Fast to Deploy** – A fully operational PKI can be up and running within days.
- **Low Cost of Ownership** – Reduce cost by using a fully managed service with minimal integration effort delivered through a highly redundant infrastructure, ensuring complete business and application continuity.
- **Scalability** – Managed PKI service scales smoothly from hundreds to millions of users. Companies pay only for the number of digital certificates required.
- **Open PKI** – Built on open standards to ensure maximum flexibility and does not lock you in any proprietary software.
- **Policy & Risk Management** – Our processes meet the highest standards, supported by liability sharing and insurance protection.
- **Secure, Reliable Operations** – We offer binding service-level agreements backed by high-security facility with specially trained, screened personnel, redundant systems, customer support for mission-critical PKI needs, and full audit.

Certification Authority
The Managed PKI service provides advanced web-based configuration wizards, administration and support tools, report generators and application integration modules to give an enterprise full control over its CA and to provide the critical link to our processing centers. The Managed PKI service capabilities provide full support for end-user registration and certification renewal with screens customized to an organization's specific look and feel for each application.

Registration Authority
Management of the lifecycle process for enrolling, approving, revoking and renewing certificates is performed easily through the our Managed PKI Control Center, giving you full control of the registration and authentication process.

With Managed PKI service you can also distribute registration authority (RA) functions such as certificate approval, revocation, audit and day-to-day management to unlimited number of administrators, providing for complete separation of administrative roles. With Managed PKI service, there is no single point of control for all aspects of defining, approving and revoking user keys and certificates, minimizing the risk of security breaches. Our Managed PKI service also provides customers with extensive audit trails and reporting capabilities along with auditable security practices – all features which support non-repudiation of certificate-based transactions.

Automated Administration Toolkit
The Managed PKI Automated Administration Toolkit automates the registration authoring functions, allowing transparent authentication and revocation of users or devices directly from pre-existing administrative systems or databases, rather than requiring manual authentication for each certificate application.

Key Management
The Key Manager and Key Recovery Service in Managed PKI allow for centralized key generation, private key backup and distributed key recovery to ensure maximum security and protection of your private keys. Dual key-pair generation is also supported, which allows for the separate issuance of encryption and signing key pairs.

24/7 Data Center Operations
The trustworthiness, reliability and value of your PKI and digital certificates are totally dependent on the security and management of your CA. Every Managed PKI implementation is linked to our high availability data centers for certificate processing, database backup, and customer support.

Our data center is equipped with state-of-the-art physical and network security, fault tolerant computing and telecommunications systems and redundant power systems. The Managed PKI customers control the initial setup and day-to-day administrative tasks of their PKI while MSC Trustgate handles all system provisioning and provides contractual guarantees on availability, security and response time.

Fast Implementation, Easy Administration
The Managed PKI service allows enterprises to quickly, securely, and cost-effectively issue digital certificates not only to employees, customers, and business partners, but also to Web services applications and network devices such as servers, routers, and firewalls.

Managed PKI Features

Comprehensive functionality
- Centralized, auditable root key generation
- Dual key-pair generation allowing the separate issuance of encryption and signing key pairs.
- International support for UTF-8 encoding enable the display of digital IDs in non-ASCII characters

Local Hosting
- Customer may localize, brand and host end-user enrollment pages

Full certificate lifecycle management
- Control Center which gives enterprise administrators full control over enrolling, approving, revoking, and renewing digital certificates.

Flexible authentication methods
- Manual authentication
- Passcode authentication
- Automated authentication

Common authentication mechanism for multiple applications:
- Trusted messaging (Microsoft Exchange, Lotus Notes)
- Secure Virtual Private Network (Checkpoint, Cisco, Nortel)
- Support for Wireless LAN via EAP-TLS
- Two-factor authentication (Aladdin, Authenex, ActivCard, Schlumberger)
- Integration with smart cards, USB tokens, Trusted Platform Modules on Intel Centrino based PCs

Support Standard
- Certification Type: S/MIME, SSL, and IPSec
- Industry standards: X.509v3, LDAP, and PKCS 7, 10, and 12
- Operating systems: Windows, Solaris, and AIX
- Browsers: Internet Explorer and Netscape

Certification Authority
- MSC Trustgate hosts and operates the CA infrastructure on behalf of the customers
- 24*7*365 Data Center operations
- Disaster recovery

MSC Trustgate.com Sdn Bhd (478231-X)
CA License No. LK 0022000
Ground Floor, Belatuk Block, Cyberview Garden, 63000 Cyberjaya, Selangor, Malaysia
Telephone: +6 (03) 8318 1800 Facsimile: +6 (03) 8319 1800 E-mail: sales@msctrustgate.com
Web site: www.msctrustgate.com