NETRUST
YOU CAN BE SURE

Managed PKI & Certificate Services

Security on the Internet is a key issue for organisations trying to strategically leverage the benefits of the web. Public Key Infrastructure (PKI) is recognised as the best solution for securing transactional information for privacy, integrity and non-repudiation. Today, organisations can choose either to use the services of a Public Certificate Authority (CA) or subscribe to a Managed PKI service to issue Digital Certificates that are branded in their own name.

Dedicated, Highly Customisable PKI

Recognising that the strong desire for organisations to set up an in-house CA that issues Digital Certificates under their own brand name is thwarted by the cost, time and expertise needed to deploy and manage a solid PKI, Netrust offers an industry-leading Managed PKI Service that allows organisations to reap the benefits of a dedicated, highly customisable PKI within a faster time and with lower financial and manpower commitments. Netrust Managed PKI Service is an outsourced Certificate Authority (CA) solution architected to enable organisations to issue and manage certificates throughout an organisation - employees, partners and customers, while leveraging on the strengths of a publicly trusted CA to undertake the back-end day-to-day processing out of a secure data centre. Organisations can then focus on its core competencies, and yet retain complete control of the certificate issuance and management processes.

How It Works

The customer organisation leverages the robust CA infrastructure that Netrust uses to deliver its CA service. Netrust provides the technical expertise in the planning, deployment and operations of the CA. The customer organisation runs the registration authority (RA) function. The verification, registration and issuance of the certificates to clients, partners and employees are handled by the customer.

Key Benefits

- Customise a private CA with own branding
- Reduce reliance on organisation's in-house IT resources to maintain the CA
- Utilisation of Netrust's high availability services
- Rely on Netrust's world-class facilities in housing the CA
- Fast time to market for PKI implementation

The Netrust Advantage

Netrust is the first public CA in Asia and the only IMDA-accredited CA in Singapore. It has been providing digital ID certificates since 1997, and the certificates are widely used for secure authentication, secure email, secure VPN, digital signing and other applications. Netrust's CA services, processes and infrastructure are audited against stringent standards set by the Controller of CA, Singapore. Netrust brings knowledge, vast experiences and operational efficiency to provide a leading Managed PKI solution that will satisfy the needs of businesses. Its team of PKI technology and CA systems experts, with deployment experience across all verticals, ensures that its customers reap the benefits of a Managed PKI service that can meet and exceed today's Enterprise PKI requirements.

USE PUBLIC CA CERTIFICATES

Use the services of a Public CA to issue certificates to clients, partners and employees and ride on the legality and security guaranteed by the use of an Accredited CA such as Netrust. For those organisations that prefer a totally outsourced approach, this is the best option.

VS

SUBSCRIBE TO A MANAGED PKI SERVICE

Set up their own CA to issue Digital Certificates to clients, partners and employees. It might be strategically important for certain organisations to host their own CA. However, the associated skill sets for day-to-day management of the CA may not be available to the organisation.

ONE IDENTITY, MULTIPLE APPLICATIONS

A comprehensive PKI enables the use of encryption and digital signature services across a wide variety of applications, thereby allowing organisations to achieve the goal of establishing and maintaining a trustworthy networking environment.

Email Encryption

Encrypted email has become an operational necessity in today's competitive digital business environment. Email encryption protects private, sensitive and valuable information communicated via email.

File Encryption

File encryption provides security for files that reside on media, in a stored state. These are files that are resting on our hard drives, USB drives or any other type of digital media storage. Those are files that are usually not meant to be sent through network, they are stored locally, being encrypted and temporarily decrypted while being used and then encrypted again after we finished using them.

VPN Security

VPN security is central to network security. VPNs allow an organisation to easily build, manage and operate low-cost private networks using the Internet to connect mobile and remote workers, remote offices and branch offices more efficiently. VPNs provide a door from the Internet into the corporate network and all its resources. The security of the network is only as strong as the method used to identify the users or devices at each end of the communication.

Wireless Security

Wireless security is also a requirement for network security. Wireless access points provide employees with anywhere, anytime access to networked resources. Unless properly protected with wireless security, those resources can also be accessed by anyone within range of the access point.

Windows Logon

When you login to your desktop, you not only have access to the resources and information stored on the computer, you also open a door to the corporate network and its data and applications. The security of the desktop and the network is only as strong as the method used to identify the users who log on to it. Organisations need to consider increasing the protection of their corporate resources by improving the mechanisms for user authentication at the time of desktop login.

Digital Signing of Documents

Enabled by proven public key infrastructure (PKI) technology, digital signatures are widely recognised as a best practice for providing digital verification of electronic transactions. Digital signatures provide "non-repudiation" — the ability to identify the author and whether the document has been changed since it was digitally signed. This functionality is particularly useful for workflow processes where one or multiple approvals are required, such as supply-chain management or financial management. Digital signatures provide confidence to customers, citizens and consumers that the material actually came from and are signed by the originating organisation.

Mobile Device Security

To effectively mitigate risk, enable true efficiency and satisfy customers in the mobile environment, organisations must properly secure mobile devices and identities — but in a way that minimises user barriers and frustrations. Once secured, organisations then have the opportunity to leverage mobile devices to actually improve security in other parts of the business.

ABOUT NETRUST

Netrust is Asia's first public Certificate Authority (CA) and Singapore's only IMDA-accredited CA. Established in 1997, it has been providing digital ID certificates widely used for secure authentication, secure VPN, secure email, digital signing and other applications. Private sector companies and Government agencies such as Building and Construction Authority, Singapore Land Authority and Land Transport Authority employ Netrust's PKI solution in their environment to enhance security and convenience, and to safely complete their electronic transactions on the Internet.

NETRUST PTE LTD
19 Tai Seng Avenue #05-01 Singapore 534054
Tel: +65-6212-1388 www.netrust.net infoline@netrust.net

NETRUST PHILIPPINES CORPORATION
Unit 1, 24th floor, Zuellig Building, Makati Avenue corner Paseo De Roxas, Makati City, Philippines 1225
Tel: +63-2-5310-2464 www.netrust.com.ph sales@netrust.com.ph

Updated 22.09.2025