# SSL Certificates
## Secure your website with Netrust

SSL certificates are one of the most important components of encrypting website data and making online transactions secure. To ensure the safety of customer and company sensitive information, and the security of financial transactions, it is crucial that organisations select and implement the right SSL certificates on their Web servers.

Netrust offers a comprehensive range of SSL certificates from leading Certificate Authorities (CAs) to secure online transactions. As Singapore's only IMDA-accredited CA, we provide end-to-end support, ensuring smooth SSL lifecycle management and rapid verification.
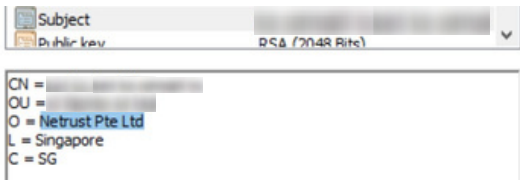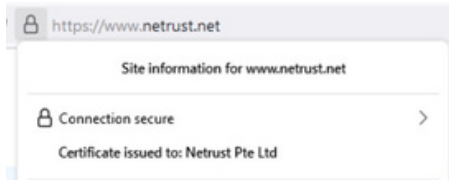
## Secure Sockets Layer (SSL) Certificate



SSL certificates are an essential component of the data encryption process that makes Internet transactions secure. The SSL certificate's job is to initiate secure sessions with a user's browser via the SSL protocol. This secure connection cannot be established without the SSL certificate, which digitally associates company information to a cryptographic key.

## The Netrust Advantage

At Netrust, we provide more than just SSL certificates. Our unique value lies in our:

1. **Accredited CA Expertise:** Netrust is not just an SSL provider; as Singapore's only IMDA-accredited Certificate Authority (CA), we bring unparalleled experience, expertise, and a proven track record.

2. **End-to-End SSL Support:** From issuance to deployment, we support the full SSL lifecycle.

3. **Dedicated SSL Team:** Specialised experts ensure seamless assistance before and after purchase.

4. **24/7 Local Support:** Round-the-clock local support for enterprise customers, including on-site assistance.

5. **Fast & Smooth Verification:** Local verification team ensures quick and efficient certificate issuance.

# Types of SSL Certificates

| Features | Organisation Validated (OV) | Extended Validated (EV) |
|---|---|---|
| **Validation Method** | Confirms domain control and vets website owner's basic business identity | Confirms domain control and performs extensive vetting of website owner's organisation identity, incorporation and authority |
| **Identity Assurance** | Organisation name in certificate  | Organisation name in certificate and web browser  |
| **Benefits** | Provides a reasonable identity assurance to site visitors | Strong identity assurance & better brand protection |

# Web-Based Certificate Management

Netrust's SSL certificates come with a user-friendly, web-based certificate management tool. This platform allows you to efficiently manage all of your SSL certificates at any time, from any location.

**Key Features:**

**Convenient Expiration Notifications**
Avoid system outages and accidental certificate expirations with automatic multi-person, multi-level expiration notifications

**Automation**
Save time and prevent errors with auto-installation tools, including Ansible (deploy TLS/SSL certificates at scale) and ACME for Web servers.

**API Integrations**
Leverage our RESTful API for your custom application or seamlessly connect with Azure Key Vault or Certificate Lifecycle Management tools like Venafi.

**TLS/SSL Server Test**
Tests your servers' TLS/SSL configuration to identify and automatically fix problems.

**ITMS Integrations**
Manage the SSL/TLS certificate life cycle in ServiceNow.

**World-Class Support**
TLS/SSL certificates are backed by Netrust's local expert and highly rated support team who is available onsite, by phone or email 24/7.

# Code Signing Certificates

Code signing is the method of using a certificate-based digital signature to sign executables and scripts in order to verify the author's identity and ensure that the code has not been changed or corrupted since it was signed by the author.

**Microsoft Smartscreen Filter**
Build a positive SmartScreen Application Reputation at twice the rate of unsigned applications.

**Third-Party Integrations**
Integrate our code-signing certificates with most third-party development tools.

**Unlimited Signing**
Identify document tampering with clear visual indicators.

**Timestamping**
Verify when code is signed and determine whether the signature is valid.

**Identified Publisher Status**
Increase user confidence and trust and avoid "Unknown Publisher" security warnings.

**Warning Box Reduction**
Removes warning message pop-ups during the installation process.

## Types of Code Signing Certificates

| Features | Organisation Validated (OV) | Extended Validated (EV) |
|---|---|---|
| Supports Windows kernal mode signing | Not Applicable | Vista, Windows 7, Windows 8 and 8.1, Windows 10 |
| Information displayed on certificate | Organisation, Location | Organisation, Location, Jurisdiction, Type of Organisation |
| Supported platforms | Authenticode, Java, Adobe Air, Microsoft Office, Microsoft VBA, Mozilla Objects | Authenticode, Java, Adobe Air, Microsoft Office, Microsoft VBA, Mozilla Objects |

## 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.