MELBOURNE IT
DIGITAL BRAND SERVICES

SSL Digital Certificates

World-class Web protection made simpler

SSL Certificates from Melbourne IT DBS

VeriSign Trusted

thawte™ it's a trust thing

GeoTrust

RapidSSL®

COMODO Creating Trust Online®

Protecting Online Transactions, Information, Brand Value, and Privacy

Secure Sockets Layer (SSL) security is the most widely deployed security protocol used on the Web today. SSL serves two key functions: authentication of the entity that owns the Web site a user will communicate with, and encryption of the data transmitted between a Web site and a user's browser. SSL Certificates ensure confidentiality and data protection throughout an online transaction.

Every business vertical or industry—from banking to retail, travel, financial services, healthcare, government, education and other—needs SSL Certificates to ensure the user that their personal information will be transmitted securely. Data being transmitted unencrypted can be easily intercepted by a third party and used for illegal or unscrupulous purposes. To date, SSL is the only scalable way to ensure a secure method of data transmission.

How SSL Works – Authentication and Encryption

An SSL session is initiated through the use of public and private key pairings. The SSL Certificate contains a private key, which is stored on the Web server and kept safe by the company that owns the SSL Certificate. Each SSL Certificate will have its own private key.

When a user connects to an SSL session, the server will identify itself by issuing a public key, which is unique to that user session. The browser will use this public key to encrypt, in real time, what the user is sending. This encryption uses a complex algorithm to encode the information. The only way to decode this information is with the private key. This forms the basis of data integrity and privacy necessary for e-commerce and other transfers of personal and confidential information.

There are different types of encryption for different types of SSL Certificates. The level of encryption is determined by what the browser is capable of, with 128-bit or 256-bit encryption being the most common today. The padlock icon and "https" proceeding the URL that are visible in Web browsers are the common visual cues that an SSL session is taking place and the transmitted information is being encrypted.

The browser also checks to make sure the certificate was issued by a trusted Certificate Authority, or CA. Prior to issuing an SSL Certificate, and depending upon the type of SSL certificate, a CA will perform a number of checks to confirm the identity of the organization requesting the certificate. These checks include: confirming domain ownership, confirming that the company is a legal entity, and confirming that the person requesting the certificate is authorized to do so. Different CAs will offer different levels of authentication. Some will complete full organizational audits while some will only verify domain ownership. As a result of this lack of consistency in how CAs authenticate a business and issue certificates, new types of SSL Certificates have entered the market that follow standards-based authentication protocols and display additional visual cues.

High Security Features for Specific Requirements – Extended Validation and Server-Gated Cryptography

Businesses with high-profile brands are increasingly using SSL Certificates with Extended Validation (EV). EV SSL Certificates provide users with visual confirmation that a Web site is trusted and secure by displaying the address bar in green. A padlock icon and "https" before the URL is also displayed, as in normal SSL environments, showing the user that the browser connection to the server is now secure. The Web site owner's legally incorporated company or organization name is displayed in the green address bar, adding an additional visual cue for the user to know who they are transacting with. EV SSL is a standard that came about from a group called the CA/Browser Forum, which developed authentication standards CAs must follow to issue certificates that will include these additional visual cues intended to inspire more user trust and confidence.

Companies that accept credit card, debit card, or other types of online payments; allow network access to financial account information; transmit healthcare or insurance information; or must adhere to specific industry or government requirements, use SSL Certificates with Server-Gated Cryptography (SGC). Encryption levels for non-SGC enabled SSL Certificates are specific to the browser. There are still browsers in use that can only encrypt at a 40-bit level, which is considered very weak and can be broken in a matter of minutes with today's computing power. SGC allows these older, legacy browsers to step up to this strong level of encryption for that session. This allows business owners the peace of mind to know that virtually all of their SSL sessions will be encrypted with at least a 128-bit level of encryption, rather than rely on the users' individual browser capabilities.

Why Buy SSL Certificates from Melbourne IT Digital Brand Services?

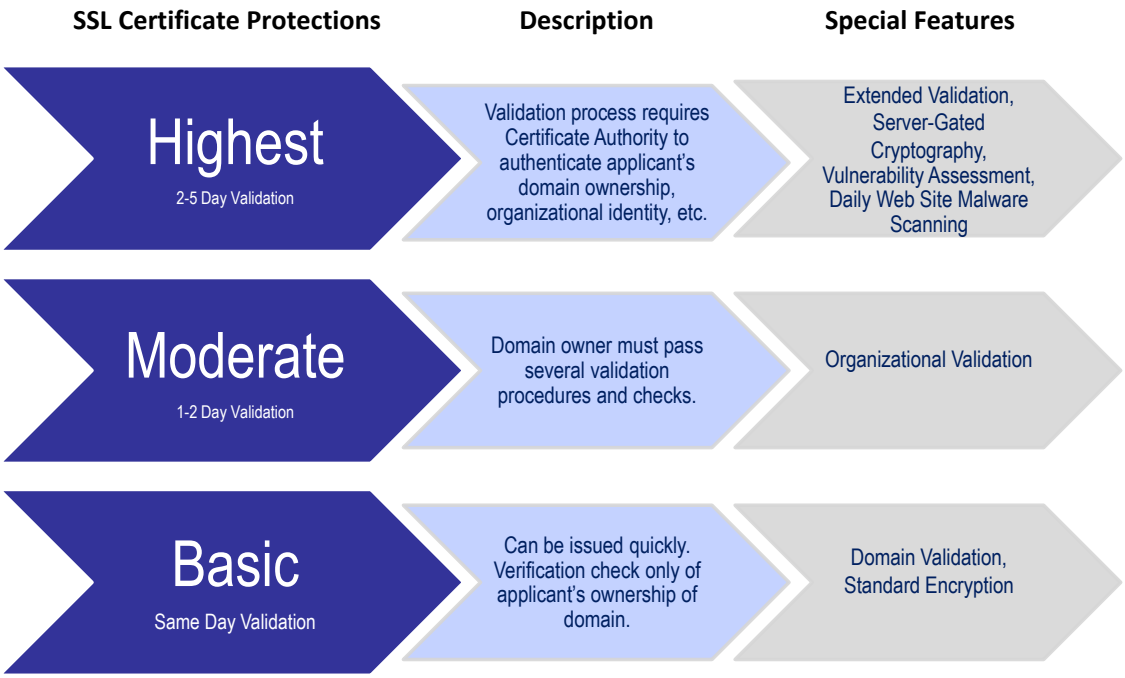
Search for "SSL Certificates" online and you will see a wide array of brands. Melbourne IT DBS offers SSL Certificates from the company with the most recognized and respected online symbol of trust for SSL and many other Web-related services, Symantec. We also have diverse products from other prominent SSL vendors Thawte, GeoTrust, Rapid SSL and COMODO.

As the leading global reseller of Symantec SSL, with a global network of offices and specialists, we have the technical expertise and domain experience to help you navigate the SSL market. Our SSL offerings are part of our effort to help clients consolidate multiple site-related services under a single vendor to reap maximum value, save time, and lower their overall costs.

Here's how we do just that:

SSL Certificate Choice and Management Made Easy

Many organizations have multiple Web sites. Some are customer-facing, others are intranets. It is often found that a mix of different brands of SSL Certificates is needed. Some sites may require a higher level of trust and therefore need the green bar EV SSL provides or a highly recognized trust mark. However, in some cases you may not require the enhanced features and a heightened sense of trust, and a less recognized brand may fit your strategy better.

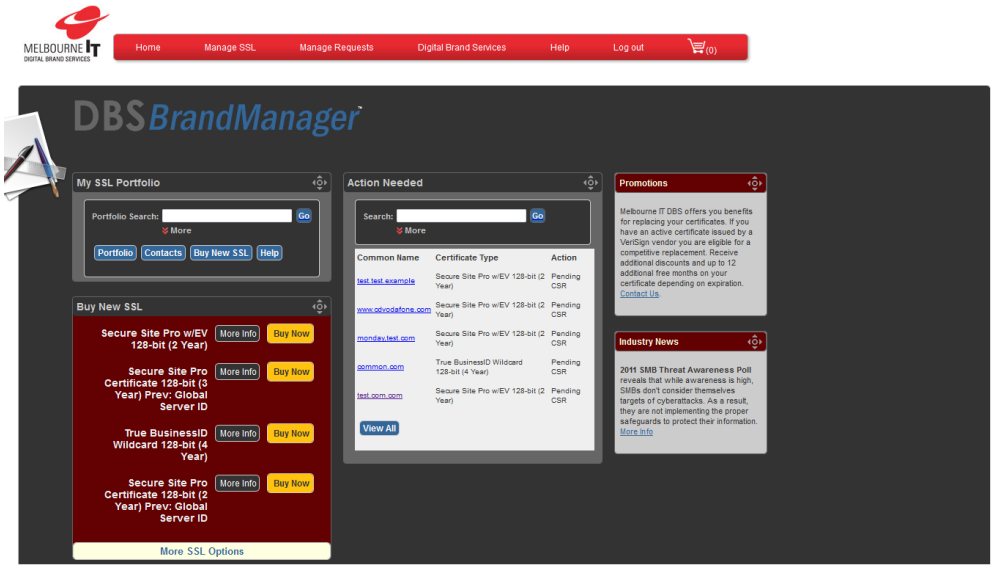


All too often, however, expensive high-security SSL Certificates are purchased for all needs due to a lack of understanding of different types of certificates and their costs. Shopping for SSL Certificates can be very confusing, especially as the technology continues to evolve.

That's why Melbourne IT DBS has made it simpler than ever to shop for SSL Certificates. Our user-friendly online SSL Manager portal helps lead you to the right SSL Certificate or mix of certificates. Now you can get better overall value for your money by purchasing the right certificate to match your specific needs.

SSL Manager also assists you in managing your SSL Certificates. You can purchase or renew certificates quickly and easily. Reminders help ensure that your certificates do not expire, causing error messages that erode user trust.

Additionally, SSL Manager allows you to upload all SSL Certificates within your environment, regardless of where they were purchased, in order to track when certificates need to be renewed, all within one portal. This eliminates the need to have multiple logins across multiple platforms to manage all of your SSL needs. The portal also handles registration for domain names and other services. It's a powerful, multipurpose dashboard to simplify the management of your Web properties.



KEY DIFFERENTIATORS

Expertise

Melbourne IT has the technical expertise and domain experience to help our customers navigate the SSL market to get better overall value by purchasing the right certificate to match their needs.

SSL Manager Portal

Our user-friendly online portal makes purchasing and renewals easy. Upload and manage information on all certificates, regardless where they were purchased.

Variety of Certificates

Shop for certificates from the most respected online symbol of trust for SSL, Symantec, along with other diverse products.

24 x 7 Support

Melbourne IT provides around-the-clock, global support in over 30 languages.

Take the first step today! For more information about our Digital Brand Management Services, please visit us at www.melbourneitdbs.com or email info@melbourneitdbs.com.

www.melbourneitdbs.com

MELBOURNE IT
DIGITAL BRAND SERVICES

Other Online Brand Services from Melbourne IT DBS

Domain Name Monitoring

Domain Name Monitoring services give companies visibility to new domain name registrations to identify infringing, fraudulent and even competitive activity. Monitoring services provide notification and alerts of new domain name registrations for both identical and similar gTLDs and ccTLDs that may infringe on current registered marks. Optional email and website monitoring services can add a greater level of risk detection. Detailed reporting of the monitoring activity lists registration activity and published contact information to provide clients with documentation to support any necessary responsive action.

Comprehensive Portfolio of Services

Our monitoring services are configurable to search email and websites for possible brand infringement, negative sentiment, and phishing and counterfeiting activity. Web crawlers scan the Internet looking for matches and modifications of client defined criteria that can include: brand names, logo matches, meta tags, keywords and phrases, links to other web pages and deep links – links two to three levels deep in a site. The data is graphically represented through our online portal where reporting sensitivity can be adjusted by the client as necessary.

Online Enforcement Services

Our Online Enforcement Services allow companies to take the appropriate action to protect their brands and minimize the impact of infringement. Monitoring service reports can be augmented with detailed investigation reports as evidence to support legal counsel action. Our in-house team of advisors can assist in developing DRP and UDRP case actions, and handle effective site (and phisher account) shut down and domain name recovery strategies and tactics. The team can also assist with discreet negotiations to proactively acquire domain names on the best possible terms for clients.