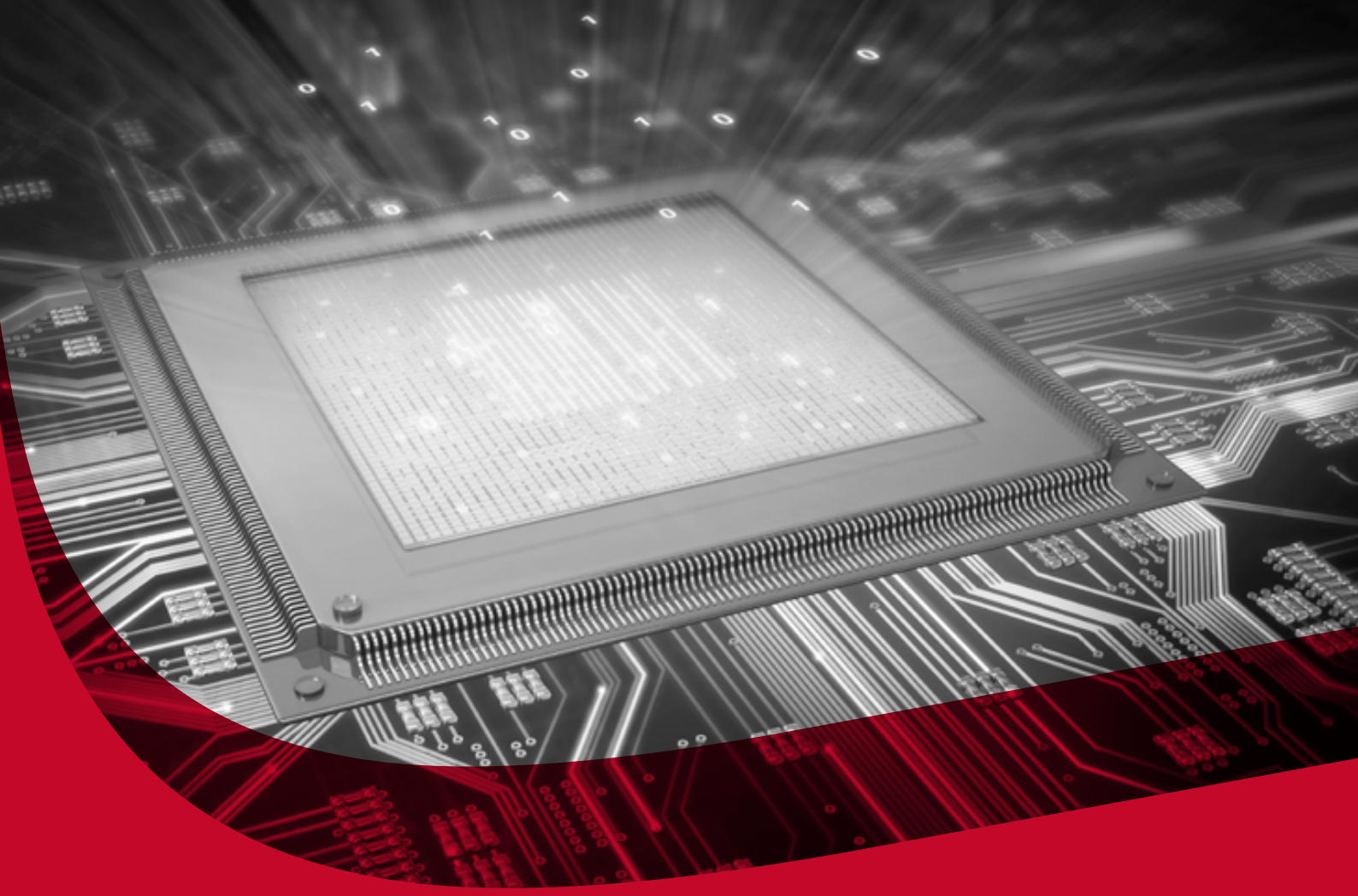


Comodo 2048 bit SSL Certificates

Security for your online business now and long into the future

COMODO
Creating Trust Online®

Today, online commerce is worth over US $1 trillion and continues to grow at a substantial rate. SSL Certificates are a cornerstone of this trade because they help establish trust and security in online transactions. The security aspect of an SSL certificate is essentially derived from its ability to strongly encrypt the data that is passed between the 'client' (your customer's browser) and the 'server' (your website's payment page). As such, you may be startled to know that the protection level of SSL certificates offered by many CA's is no longer deemed adequate. Why? Because the increasing sophistication of hackers means that certificates signed with 1024 bit keys could be vulnerable to attack in the near future. Recommendations by influential authorities such as the National Institute of Standards (NIST) and the Certificate Authority/Browser forum state that all certificates should be of 2048 bit key length after 2010.

But how does this affect your business, and shouldn't you just trust your SSL provider to look after this? To answer that question, we need to look a little more closely at the way SSL certificates work.

2048 Bit Keys – The Official Line

NIST Recommendation
The National Institute of Standards and Technology (NIST) of the US Government has stated that certificates signed with 1024 bit RSA keys should not be used to protect data after 2010. They recommend that all root certificates after this date should be of at least 2048 bit key length.

CA/B Forum
The Certificate Authority/ Browser (CA/B) forum has mandated that all Extended Validation (EV) certificates with a life-cycle past December 31st, 2010 be 2048-bit.

Certificates, Online Trust and Key Sizes – an overview

The defining function of an SSL Certificate is to establish trust between a website and the end user. For example, the relationship between an e-commerce vendor selling goods or services from their website and the customer using his or her credit card to purchase these goods online.

A Certificate Authority (CA) such as Comodo CA will sign the SSL certificates it issues to website owners with their private key. The strength of this key (1024 or 2048 bit) determines how difficult it would be to compromise the certificate. But, for the website's certificate to operate correctly, there is a reciprocal client side requirement - the Internet browser that the visitor is using MUST physically contain the Certificate Authority's 'root certificate'. Each root certificate binds the identity of the signing organization (the CA) to the public key of that root certificate. This public key is required to successfully decrypt and authenticate any website certificates that have been signed the corresponding private key of the CA. Certificate Authorities proactively supply Internet browser vendors with their roots for inclusion in the

browser's 'certificate store' - an internal repository of root certificates that ships with each browser.

The need for certificate ubiquity

Once in this store, the root certificate is used to check and verify the SSL certificate on the merchant's website. If a root key is not available, the authentication process cannot be completed and the browser strongly warns the user not to continue or submit confidential information such as credit card details. It is therefore in the interests of every CA to ensure that their root keys are in the certificate stores of as many browsers as possible. This is known as certificate 'ubiquity' – and this need for ubiquity is where the key strength issue begins.

As strong as the weakest link

Because the requirement to sign a root certificate with 2048 bit keys is quite recent, many CA's do not have their 2048 bit root certificate in all popular browsers. To get around this they employ a system known as 'cross-signing' - signing the 2048 root certificate with another root certificate that happens to be included in the browser in question. This 'daisy chaining' of an unrecognized root certificate to a recognized root certificate is an industry standard practice that allows the CA to complete the chain of trust and thus avoid the end user seeing any error messages. Unfortunately, many of the certificates used to cross-sign are of the older 1024 bit key strength – and if you cross-sign a 2048 bit certificate with 1024 bit certificate in order to facilitate an SSL connection then you also weaken the security of the whole connection back down to 1024 bits – fundamentally undermining the reason for 2048 bit certificates in the first place. This distinction is most relevant when considering that it would be possible to break a 1024-bit key much, much more quickly than a 2048-bit key. This is so important that, as mentioned earlier, new SSL certification standards developed by major browser providers like Microsoft and leading CA's identify 2048-bit CA key sizes as the new standard from 2010 onwards.

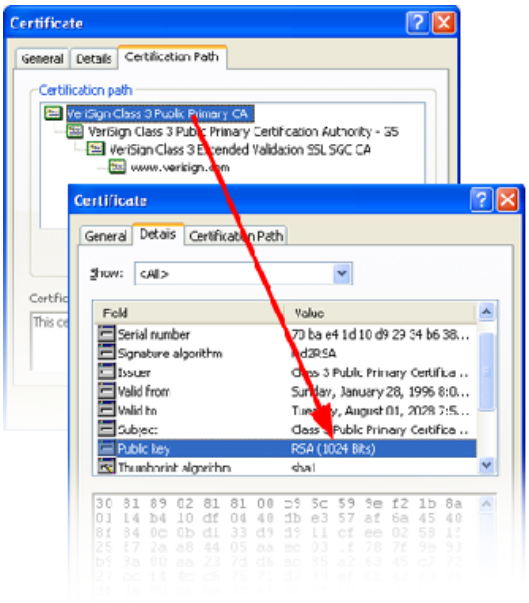
sales@comodo.com 1 (888) 266 6361

Comodo Certificates are 2048 Bit Ready

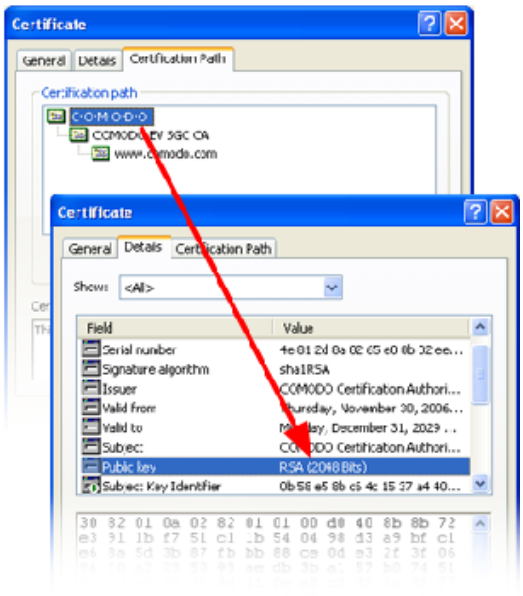
Comodo anticipated the need for longer root keys at the beginning of the millennium by embedding its 2048 bit root keys into browsers when very few other Certificate Authorities were doing so – including VeriSign. The advantage now is that Internet users with older browsers can use Comodo's highly secure 2048-bit certificates with no error messages – meaning our SSL customers are able to cover the maximum possible customer base and provide the very highest levels of SSL security.

How to tell if a certificate was issued from a 1024-bit root

You can view the certificate of a website by clicking on the yellow padlock symbol when at the website and then selecting "View Certificate". Look for the signature value of the key used to sign the certificate and the key used to request the certificate. If the root used to sign the certificate was not at least 2048-bit in length then it could be vulnerable to attack. Be diligent and make sure the certificate type you require is signed by a Certificate Authority with a 2048-bit root.



The certificate chain for *https://www.verisign.com* as viewed in Internet Explorer 6 proves the root certificate behind their EV certificate uses only 1024 bit keys. Viewed in the same browser, the EV root certificate for *https://www.comodo.com* is shown to use keys of the NIST recommended 2048 bit key length.



Future-Proof your business with Comodo SSL Certificates

Comodo is there to help online businesses make the transition to 2048 bit certificates – and save money in the process. Over 10 years of experience at the forefront of PKI innovation has led to the development of a diverse range of certificates that dovetail perfectly with the real world requirements of online business.

With Comodo, you can stay one step ahead without any extra effort using a provider you can trust for years to come.

What types of SSL Certificates are available from Comodo's 2048-Bit Root Keys?

Comodo offers a comprehensive range of 2048 bit certificates covering the full spectrum of enterprise needs – including single domain, multi-domain, wildcard and EV certificates. See the next page for closer look at what we have to offer.

sales@comodo.com
1 (888) 266 6361

Comodo's range of 2048 bit SSL Certificates

Extended Validation SSL Certificates

Provide the highest levels of encryption, security and trust to your customers and improve conversion rates. EV certs reassure visitors that it is safe to conduct online transactions by turning the address bar green on popular browsers such as Internet Explorer Firefox and Opera.

- **Validated to EV guidelines to provide the highest levels of SSL security and trust**
- **Boost consumer confidence with the Green Address Bar**
- **Helps reduce shopping cart abandonment and improve customer conversion**
- **Free EV Corner of Trust website logo and $1,750,000 warranty**
- **2048 bit ready**

Organization Validation SSL Certificates

OV certificates include full business and company validation from a certificate authority using currently established and accepted manual vetting processes. Each certificate comes with a warranty, free TrustLogo and is 2048 bit ready.

- **Full range of OV certificates de sign to meet the needs of all business sizes**
- **Recognized by 99.9% of all Internet browsers**
- **Secures both domain.com and *www.domain.com***
- **Warranties range from $10,000 right up to $1,000,000**
- **Full telephone and email support, 30 day refund and unlimited re-issuance policies**
- **2048 bit ready**

Wildcard SSL Certificates

Allow web-hosts and enterprises to secure unlimited sub-domains on a single certificate. Wildcard's provide a very cost effective alternative to single certificates and help simplify the certificate management processes.

- **Less to worry about – one certificate secures unlimited sub-domains**
- **Big savings over the cost of single certificate purchases**
- **Trusted by 99.9% of all Internet browsers**
- **$250,000 warranty, fully supported, unlimited reissuance**
- **Free Corner of Trust website logo**
- **2048 bit ready**

Multi–Domain SSL Certificates

Designed for MS Exchange and Office Communications Server 2007, UCC's Secure multiple domains from a single certificate using the Subject Alternative Name field.

- **MDC's allow you to secure up to 100 different domains on a single certificate - representing a solid investment in your web site's security and a very cost effective alternative to individual certificate purchases.**
- **Save hundreds or thousands of dollars over the cost of individual certificates**
- **Simple and convenient - only one certificate to manage for all your domains**
- **Base MDC secures 3 domains with additional domains available at hugely discounted rates**
- **Domains can be added or replaced at any time during the certificate life cycle**
- **2048 bit ready**

Comodo SSL Certificate - Supported Applications, Operating Systems and Platforms

Extended Validation Browsers

- Microsoft Internet Explorer 7+
- Opera 9.5+
- Firefox 3+
- Google Chrome 0.3.154.9 +
- Apple Safari 3.2 +
- Apple iPhone 3.0 +

Web Browsers (SSL/TLS enabled)

- Microsoft Internet Explorer (IE) 5.01+
- Mozilla Firefox 1.0+
- Opera 6.1+
- Apple Safari 1.0+
- Google Chrome
- AOL 5+
- Netscape Communicator 4.51+

sales@comodo.com 1 (888) 266 6361

- Red Hat Linux Konqueror (KDE)
- Microsoft WebTV
- Camino
- Konqueror (KDE) 2.0.0 +

Email Clients (S/MIME)

- Microsoft Outlook 9.0+
- Microsoft Entourage (OS/X)
- Mozilla Thunderbird 1.0+
- Qualcomm Eudora 6.2+
- Lotus Notes (6+)
- Netscape Communicator 4.51+
- Mulberry Mail
- Apple Mail
- Mail.app
- Windows Mail
- The Bat
- Major Operating Systems
- Microsoft Windows XP, Vista and 7 (all versions inc 32/64 bit)
- Apple MAC OS 9.0+ (circa 2002), includes 10.5.X and 10.6.X
- All Major Linux Distributions (Debian, Ubuntu etc)

API Support within Hosting Control Panels

- WHMCS
- Ubersmith

Mobile OS, Micro Browsers, Handsets & Game Consoles

- Android (inclusion carrier specific)
- Apple iPhone, iPod Safari
- Microsoft Windows Mobile 5/6
- Microsoft Windows CE 4.0
- Microsoft Internet Explorer Pocket PC 2003
- Microsoft Internet Explorer Smartphone 2003
- RIM Blackberry 4.3.0
- NTT / DoCoMo
- SoftBank Mobile
- KDDI
- Brew
- PalmOS 5.x
- Netfront 3.0+
- Opera 4.10+
- Openwave mobile browser 6.20+
- Major Operators inc. Vodafone, Orange, AT&T
- Major Handset providers SonyEricsson, Nokia, Alcatel & Palm (S40/S60/S80/OSSO) based Handsets from 2002
- Sony PlayStation Portable
- Sony PlayStation 3
- Nintendo Wii

Application Suites

- Microsoft Authenticode & Visual Basic for Applications (VBA)
- Adobe AIR
- Sun Java JRE (1.4.2 Update 16+, 5.0 Update 13+, 6 Update 3+)
- Mozilla Suite v0.9.8+
- SeaMonkey
- OpenSSL.org's OpenSSL v0.9.5+
- Google Checkout

Document Security Platforms

- Microsoft Office (Word, Excel, Powerpoint, Access, InfoPath)

For more information about Comodo SSL certificates, visit: ***www.instantssl.com***

Comodo SSL solution experts can be contacted directly by emailing ***sales@comodo.com***

sales@comodo.com 1 (888) 266 6361

About Comodo

The Comodo companies create the infrastructure that is essential in enabling e-merchants, other Internet-connected companies, software companies, and individual consumers to interact and conduct business via the Internet safely and securely. The Comodo companies offer PKI SSL, Code Signing, Content Verification and Email Certificates; award winning PC security software; vulnerability scanning services for PCI Compliance; secure email and fax services. Continual innovation, a core competence in PKI, and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo secures and authenticates online transactions and communications for over 200,000 business customers and 10,000,000 users of our desktop security products.

For additional information on Comodo – Creating Trust Online™ visit www.comodo.com

Comodo CA Limited
3rd Floor, 26 Office Village,
Exchange Quay,
Trafford Road, Salford,
Manchester M5 3EQ,
United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767

Comodo Group, Inc.
1255 Broad Street
Clifton, NJ 07013
United States

Tel: +1.(888).266.6361
Email: Sales@Comodo.com