

Stay one step ahead with Comodo 2048-bit Certificates

If you are still using a 1024-bit certificate, you may soon be vulnerable to a “brute-force attack”. An exponential trend in computer processing power has resulted in the ability for criminals to compromise 1024-bit key strength certificates. Leading cryptography organizations, including NIST, have issued recommendations for entities to upgrade to longer key lengths.

Based on these recommendations, entities wishing to keep secure for the next several years need to start using 2048-bit certificates. This is extremely important for those who purchase multi-year SSL certificates.

NIST Recommendation

The National Institute of Standards and Technology (NIST) of the US Government stated that 1024-bit certificates will soon become vulnerable. They recommend that key lengths be upgraded to 2048-bit strength by 2010. Any certificate issued with a term length past 2010 should be 2048-bit to be considered secure.

CA/B Forum

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

[Comodo has you covered now and for the next 20 years!](#)

Comodo is there to help you make the transition. Comodo readily offers and supports a variety of 2048-bit certificates. To get a Comodo 2048-bit certificate, just make sure you create a 2048-bit certificate request and you are done. With Comodo, you can stay one step ahead without any extra effort using a provider you can trust for years to come.

[How to tell if your certificate was issued from a 1024-bit root](#)

You can view the certificate of a website by clicking on the SSL Certificate indicator 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 the certificate can not be 2048-bit and will be vulnerable to brute-force attacks.

Not all CAs are issuing from 2048-bit roots. Be diligent and make sure the certificate type you require is signed by a Certificate Authority with a 2048-bit root.

[What types of SSL certificates are available from Comodo’s 2048-bit root keys?](#)

Every single one. Single domain, wildcard, EV, multi-domain SAN - every certificate Comodo offers is 2048-bit ready.

Comodo SSL Certificate Compatibility

Web Browsers:

Microsoft Internet Explorer 5.01 +
Mozilla Firefox 1.0+
Mozilla 0.6+
Google Chrome
Konqueror (KDE)
Netscape 4.77 +
Opera 7.0+
Apple Safari 1.2 +
Camino 1.0+
AOL 5+

Additional Applications:

Google Checkout
Sun Java 1.4.2
SeaMonkey
Internet Explorer 7: (Vista)
Internet Explorer 7: (XP)
Mozilla Firefox 3.

Micro Browsers /PDAs

Apple iPhone, iPod Safari 1.0+
Microsoft Windows Mobile 5/6*
ACCESS NetFront Browser v3.4 +
RIM Blackberry v4.2.1 +
KDDI Openwave v6.2.0.12 +
Opera Mini v3+
Opera Mobile 6+
Sony Playstation Portable
Sony Playstation 3
Netscape Communicator 4.51+
Nintendo Wii
NTT / DoCoMo

Email Clients (S/MIME):

Microsoft Outlook 99+
Microsoft Entourage (OS/X)
Mozilla Thunderbird 1.0+
Microsoft Outlook Express 5+
Qualcomm Eudora 6.2+
Lotus Notes (6+)
Mail.app (Mac OS X)
Microsoft / Windows Mail 1.0+ (Vista)
The Bat 1+

Application Suites:

Microsoft Authenticode
Visual Basic for Applications (VBA)
Adobe AIR
Sun Java SE 1.4.2+
Mozilla Suite 1.0+
Sea Monkey

Document Security Platforms:

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

Server Platforms:

All SSL-Capable Server Platforms

Extended Validation:

Microsoft Internet Explorer 7+ (Vista)
Microsoft Internet Explorer 7+ (Windows XP)
Opera 9.5+
Firefox 3+
Apple Safari 3.2+
Google Chrome 1+

Micro Browsers /PDAs

Apple iPhone, iPod Safari 1.0+
Microsoft Windows Mobile 5/6*
ACCESS NetFront Browser v3.4 +
RIM Blackberry v4.2.1 +
KDDI Openwave v6.2.0.12 +
Opera Mini v3+
Opera Mobile 6+
Sony Playstation Portable
Sony Playstation 3
Netscape Communicator 4.51+
Nintendo Wii
NTT / DoCoMo

Server Platforms

Apache
BEA Weblogic
C2Net Stronghold
cPanel / Web Host Manager
Ensim Control Panel
Hsphere
IBM HTTP Server
iPlanet Server / Sun One
Java Web Server (Javasoft / Sun)
Lotus Domino
Microsoft IIS
Microsoft ISA
Microsoft Live Communication Server
Microsoft SQL Server 2005
Netscape Enterprise Server
Novell ConsoleOne + Novel Webserver
OpenLDAP
Oracle HTTP Server
Plesk
Tomcat
Webmin
WebSTAR
Zeus Web Server

If you would like to discuss Comodo 2048-bit certificates with a sales representative, then contact us at 1.888.266.6361 or 1.703.581.6361 or email sales@comodo.com

About Comodo

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet, with over 3,000,000 customers worldwide. Headquartered in the United Kingdom with global offices in the US, Ukraine, and India, the company offers businesses and consumers the intelligent security, authentication and assurance services necessary to ensure trust in online transactions.

As a leading certificate authority, Comodo helps enterprises address digital ecommerce and infrastructure needs with reliable third generation solutions that improve customer relationships, enhance customer trust, and create efficiencies across digital ecommerce operations. Comodo's solutions include SSL certificates, web content authentication, infrastructure services, digital e-commerce services, digital certification, identity assurance, customer privacy and vulnerability management solutions.

For additional information on Comodo, please visit www.comodo.com

Comodo Certificate Authority

Comodo CA Limited

26 Office Village, 3rd Floor
Exchange Key, Trafford Road
Salford, Manchester M5 3EQ
United Kingdom

Tel Sales: +44 (0) 161 874 7070
Fax Sales: +44 (0) 161 877 7025
Comodo Group, Inc.

525 Washing Blvd.,
Jersey City, NJ 07310
United States of America

Tel: + 1.888.COMODO.1
email : sales@comodo.com