# SHA-2 COMPATIBILITY

## INTRODUCTION

SHA-2 is a set of cryptographic hash functions which includes SHA-224, SHA-256, and SHA-512. The 256 in SHA-256 represents the bit size of the hash output or digest when the hash function is performed. Not all software supports every digest size within the SHA-2 family.

Most browsers, platforms, mail clients, and mobile devices already support SHA-2. However, some older operating systems such as Windows XP pre-SP3 do not support SHA-2 encryption.

This article focuses specifically on SHA-256 and its compatibility with various software platforms and operating systems. As a general rule, SHA-256 is supported on OS X 10.5+ and Windows XP SP3+.
This page lists the minimum version required for SHA-2 as well as some exceptions.

## 01 BROWSER & SERVER SUPPORT

| Browser | Minimum Browser Version |
|---|---|
| Chrome | 26+ |
| Firefox | 1.5+ |
| Internet Explorer | 6+ (With XP SP3+) |
| Konqueror | 3.5.6+ |
| Mozilla | 1.4+ |
| Netscape | 7.1+ |
| Opera | 9.0+ |
| Safari | 3+ ( Ships with OS X 10.5 ) |

| Server | Minimum Server Version |
|---|---|
| 4D Server | 14.01+ |
| Amazon Web Services (AWS)[1] | *Yes* |
| Apache | 2.0.63+ w/ OpenSSL 0.9.8o+ |
| Barracuda Network Access Client | 3.5+ |
| Cisco ASA 5500 | 8.2.3.9+ for AnyConnect VPN Sessions; 8.4(2)+ for other functionalities |
| Citrix Receiver | Varies - See PDF ( FIPS 140 & SHA-2 Line ) |
| CrushFTP | 7.1.0+ |
| F5 BIG-IP | 10.1.0+ |
| IBM Domino Server[2] | 9.0+ (Bundled with HTTP 8.5+) |
| IBM HTTP Server[2] | 8.5+ (Bundled with Domino 9+) |
| IBM z/OS | v1r10+ |
| Java based products | Java 1.4.2+ |
| Mozilla NSS Based Products | 3.8+ |
| OpenSSL based products | OpenSSL 0.9.8o+ |

[1] *Although AWS is SHA-2 compatible, instances of AWS are typically Virtual Private Servers. Therefore, AWS SHA-2 compatibility is dependent on the base server platform. Other AWS applications (such as Elastic Load Balancing (ELB)) support SHA-2 Certificates.*

[2] *IBM Domino Server by itself does not currently support SHA-2 secured connections. To use SHA-2 SSL Certificates to secure your connection, you must use an HTTP proxy server that is set up to handle your incoming HTTPS requests. Domino 9.0 includes HTTP proxy server support and is configured so that you can use it with IBM HTTP Server ( https://www-01.ibm.com/support/docview.wss?uid=swg27041958 ).*

## 02 OS SUPPORT

| Operating System | SSL Certificate Minimum OS Version | Client Certificate Minimum OS Version |
|---|---|---|
| Android | 2.3+ | 2.3+ |
| Apple iOS | 3.0+ | 3.0+ |
| Blackberry | 5.0+ | 5.0+ |
| ChromeOS | Yes | Yes |
| Mac OS X | 10.5+ | 10.5+ |
| Windows | XP SP3+ | XP SP3+ (Partial) |
| Windows Phone | 7+ | 7+ |
| Windows Server | 2003 SP2 +Hotfixes (Partial) | 2003 SP2 +Hotfixes (Partial) |

*[3] To enable the same SHA-2 compatibility on Windows Server 2003 as Windows XP SP3, see KB 938397.*

*[4] To fix issues when authenticating from XP SP3 or Server 2003 to Server 2008 using SHA-2, see KB 968730.*

## 03 EMAIL CLIENT COMPATIBILITY

| Email Client | Verify SHA-2 Signed E-Mail | Sign E-Mail with SHA-2 |
|---|---|---|
| IBM Notes 9+ | *Yes* | *Yes* |
| Mac Mail on OS X 10.5+ | *Yes* | *Yes* |
| Mozilla Thunderbird1.5+ | *Yes* | *Yes* |
| Outlook 2007+ on Vista+ | *Yes* | *Yes* |

## 04 DOCUMENT SIGNING COMPATIBILITY

| Client | Verify SHA-2 Signed Document | Place SHA-2 Signature with SHA-2 certificate |
|---|---|---|
| Adobe Acrobat Pro 9+ | *Yes* | *Yes* |
| Adobe Reader 9+ | *Yes* | *N/A* |
| LibreOffice Writer 4.2 on Vista+ | *Yes* | *Yes* |
| Word 2007+ on Vista+ | *Yes* | *Yes* |

## 05 CODE SIGNING COMPATIBILITY

| Operating System | Authenticode | Kernel Mode | VBA Macros: Office 2003, 2007, 2010 | VBA Macros: Office 2013 |
|---|---|---|---|---|
| Windows 8 | *Yes* | *Yes* | *No* | *Yes* |
| Windows 7 | *Yes* | *No* | *No* | *Yes* |
| Windows Vista | *Yes* | *No* | *No* | *N/A* |
| Windows XP SP3 | *Yes* | *No* | *No* | *N/A* |

## 06 SAFENET eTOKEN / iKEY COMPATIBILITY

| eToken / iKey | Place SHA-2 Signature |
|---|---|
| eToken 5205 | *Yes* |
| eToken 5200 | *Yes* |
| eToken 5105 | *Yes* |
| eToken 5100 | *Yes* |
| iKey 4000 | *No* |

### INFORMATION ABOUT POS DIGICERT SDN BHD

With over a decade of experience, Pos Digicert strives to offer world-class security solutions technologies to help application service providers enhance their effectiveness and capabilities in addressing security challenges. Pos Digicert will continue to build on its core strength and move forward in making its mark as a trusted and reliable electronic identity and security services provider.

For more information, please visit

**https://www.digicert.com.my**