Recommendations and minimum requirement for usage of SHA-2 Digital Signature Certificates

For organizations looking to deploy SHA2 or organizations that interact with 3rd parties that will soon begin using SHA2, the following is recommended.

- If Windows XP is used in the environment, **Service Pack 3 should be deployed**. In addition to SHA2 functionality, Service Pack 3 is currently the only Windows XP service pack that is supported.
- If Windows XP systems would need to enroll in certificates from a SHA2 certificate authority**, KB 968730 should be deployed.**
- If Windows Server 2003 is used in the environment, Service Pack (1 or 2) and KB **938397 should be deployed**.
- If Windows Server 2003 would need to enroll in certificates from a SHA2 certificate authority, Service Pack 2 and KB 968730 should be deployed. If planning on deploying KB 968730, installing KB 938397 is not necessary.
- If S/MIME using SHA2 signing for the message body is needed, workstations should be upgraded to at least Windows Vista running Office 2003/2007/2010
- **Adobe acrobat 9.1**
- **Internet explorer 7 and upper version supported**
- **Outlook 2003/2007/2010 supported**

Windows supported with SHA-2

Clients - Windows XP (service pack 3) | Windows Vista | Windows 7
Servers - Windows Server 2003 | Windows Server 2008 | Windows Server 2008 R2

Software Supported:

- **Adobe acrobat 9.1**
- **Internet explorer 7 and upper version supported**
- **Outlook 2003/2007/2010**

Clients - Windows XP (service pack 3) | Windows Vista | Windows 7
Servers - Windows Server 2003 | Windows Server 2008 | Windows Server 2008 R2

Summary Chart

	Summary Chart	**XP SP3**	**XP SP3 with KB968730**	**Windows Vista, 7, 2008, 2008 R2**
Basic Functionality				
	Browsing a website using SHA2 certificate	Works	Works	Works
	Open a certificate and viewing properties	Works	Works	Works
Interactive logon and mutual TLS (client system)	Client with SHA2 certificate; server with SHA1 certificate	Works	Works	Works
	Client with SHA2 certificate; server with SHA2 certificate	Works	Works	Works
Interactive logon and mutual TLS (domain controller / IIS server)	Client with SHA2 certificate; server with SHA1 certificate	N/A	N/A	Works
S/MIME (Outlook 2003)	Validate and sign to a SHA2 certificate	Works	Works	Works
S/MIME (Outlook 2007 and 2010)	Validate and sign to a SHA2 certificate using SHA-1 for the message signature	Works	Works	Works