# Technical Advisory – SHA-256 Certificate Interoperability with select Microsoft Windows editions (KB938397)

| | | | |
|---|---|---|---|
| **Date issued:** | 05-05-11 | **Advisory sent to:** | PKWARE Technical Support, Sales Engineers |
| **Effective date:** | Immediately | **Products affected:** | • SecureZIP® and SecureZIP PartnerLink™ on Windows platforms |
| **Technical Support Ticket ID:** | N/A | **Location of completed fix:** | N/A |

**Short description of issue:** Customers moving to new digital certificates signed with the SHA-256 hashing algorithm may experience unexpected validation warnings when using these certificates on specific versions of Windows 2003 Server and Windows XP operating environments. Applying a documented Hotfix available from Microsoft will resolve this issue. Please direct customers to Microsoft Knowledge Base article KB938397. Details on this issue are available from Microsoft at this link http://support.microsoft.com/default.aspx?scid=kb;EN-US;938397.

While this issue may be experienced by SecureZIP® and SecureZIP PartnerLink™ customers on these affected platforms, no changes to PKWARE software are required. This issue affects only those operating systems referenced and does not occur on any non-Windows platforms.

**Detailed description of issue:**

Customers moving to new digital certificates signed using the SHA-256 algorithm, may experience a problem with these certificates within PKWARE products on specific Windows operating system editions. There is a documented issue with the Microsoft cryptographic libraries on 32 bit and 64 bit versions of Windows 2003 Server R2, and on 64-bit versions of Windows XP with SP2. This problem will also occur on other 32 bit Windows XP editions not running at Service Pack 3. Customers on 32-bit XP should make sure they are running Service Pack 3 for XP. Additional information on this problem is available from Microsoft under Microsoft Knowledge Base Article KB938397.

While the use of SHA-256 signed certificates is not widely seen yet, we anticipate an increasing likelihood that this may impact PKWARE customers that are looking to comply with NIST algorithm migration guidelines set to take affect by the end of 2013. Customer's using certificates signed using the SHA-256 algorithm may see these certificates appearing as invalid or as not trusted when they are used within PKWARE products. PartnerLink customers should inform their partners if they are issuing them new SDP's that use SHA-256 certificates to ensure they are aware of this Windows Hotfix.

To resolve this issue, customers need only apply the correct Hotfix available from Microsoft. Correct operation will be restored once this Hotfix is applied. Customers do not need to replace their SHA-256 certificates, nor do they need to change, or upgrade their PKWARE software to resolve this issue.

**Recommended work-around:**

There is no work-around for this issue and affected customers must obtain and install the recommended Microsoft Hotfix to resolve this issue. Refer to Microsoft KB938397 for information on how to request and apply this Hotfix (http://support.microsoft.com/default.aspx?scid=kb;EN-US;938397).

**Contact PKWARE:**

The information documented in this advisory is based on interoperability testing performed by PKWARE, using PKWARE products. For questions or additional information regarding this issue please contact PKWARE Product Support by phone +1.937.847.2687 or on the web at http://www.pkware.com/support/desktop, for more information.