EDIDEV KNOWLEDGE LETTER
March 31, 2018
http://www.edidev.com

Migrating from SHA1 to SHA256

If you haven't yet migrated your AS2 application from SHA1 to SHA256, you may very well soon be asked to. Below are the steps:

1. Purchase or create a certificate that supports SHA256, and install it on the server where your AS2 server is running. Export its public certificate, and send it to all your trading partners for them to use to encrypt AS2 messages they send you.

2. Change the code in your AS2 Server program to use by default a CSP that supports SHA256 like "Microsoft Enhanced RSA and AES Cryptographic Provider". The code would look something like below:

```
oSecurities.DefaultProviderName = "Microsoft Enhanced RSA and AES Cryptographic Provider";
```

3. Use the eSecurityConsole utility to verify where your certificate was installed and modify the following security certificate properties accordingly:

```
oSecurities.DefaultCertSystemStoreLocation
oSecurities.DefaultCertSystemStoreName
oSecurities.DefaultKeyContainer
oMdnSecurity.CertificateSignerName
```

4. At the As2 client end, you would have to obtain the public certificates (that supports SHA256) from your trading partners, and install them on the As2 client application's machine.

5. Similarly to the AS2 server, modify your code to use a CSP that supports SHA256, and modify the securities object's properties accordingly to where you installed your trading partners' certificates.

6. Lastly, change the "sha1" value in the Disposition-Notification-Options to "sha256". The header should look something like:

```
Disposition-Notification-Options: signed-receipt-protocol=optional,pkcs7-signature;signed-receipt-micalg=optional,sha256
```

*** A sample As2 client in Excel VB script (ExcelEdi850_As2) that uses SHA256 can be downloaded from http://www.edidev.com/example_business.html.

EDIDEV
"We make EDI fun!"