AS2 Signature and Encryption Algorithms for Inbound Transactions

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v7.4.11 and later

DISCUSSION

EFT v7.4.11 was updated to use the /n 2016 EDI Integrator component, which includes the option to specify allowed signature/ encryption algorithms for inbound transactions. The MDN (Message Disposition Notification) is signed using the specified algorithm. Which algorithms to use can be configured in the registry, as described below.

Available signature algorithms for inbound transactions include:

- 0 As Requested
- 1 As Requested Or SHA1
- 2 SHA1
- 3 MD5
- 4 None
- 5 SHA-256
- 6 SHA-384
- 7 SHA-512
- 8 SHA-224
- 9 As Requested Or SHA-256 (default)

Available encryption algorithms include:

- 3DES
- DES
- AESCBC128
- AESCBC192
- AESCBC256

All available algorithms except "DES" are selected by default.

To specify one or more algorithms, create the following registry settings:

HKEY_LOCAL_MACHINE\Software\WOW6432Node\GlobalSCAPE Inc.\EFT Server 7.4\

AS2 Signature and Encryption Algorithms for Inbound Transactions

Type: STRING

Value names:

- AS2EncryptionAlgorithm
- AS2SignatureAlgorithm

Restart Required: yes

Backup/Restore: yes

In the COM API, these options are configurable via the COM API properties "Signature Algorithm" and "Encryption Algorithm".

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11432/AS2-Signature-and-Encryption...