x. Data integrity and protection

S-100 Part 15 defines the algorithms for compressing, encrypting and digitally signing datasets based on the S-100 Data Model. The individual product specifications provide details about which of the elements are being used and on which files in the dataset.

x.1 Use of Compression

Information about compression is encoded in the S100_ExchangeCatalogue. It implies that either all files or none in the exchange set are compressed.

All files (or only ENC dataset files) included in a S101 exchange set are compressed in accordance with S-100 part 15. The S101ed1.CAT file shall never be compressed.

The use of compression will be encoded:

Field name	***Comments***
S100_ExchangeCatalogue	
compressionFlag: 1	Compression enabled
algorithmMethod: 1.0.0	ZIP algorithm defined in S-100 part 15 ed 1.0.0

x.2 Use of Data Protection

All ENC dataset files are encrypted in accordance with S-100 part 15. No other files are encrypted. Encryption method is AES with a 128 bit key length.

The ENC dataset files shall be compressed before they are encrypted.

An ENC cell edition and all its associated update files shall be encrypted using the same encryption key.

The use of data protection for ENC files shall be encoded:

Field name	***Comments***
S100_DatasetDiscoveryMetaData	
dataProtection: 1	File is encrypted
protectionScheme: 1.0.0	AES-128 algorithm defined in S-100 part 15 ed 1.0.0

For all other files in the exchange set shall dataProtection be 0 and protectionScheme is not used.

x.3 Use of Digital Signatures

All files included in a S-101 exchange set shall have a digital signature as defined in S-100 part 15. The digital signature value will be encoded in the S-100_DatasetDiscoveryMetaData.

For encrypted dataset files, the digital signatures must be calculated after compression and encryption. A dataset file must be authenticated before it is decrypted and uncompressed.

Since the S101ed1.CAT file is not referenced in the discovery meta data, its signature will be stored in a separate file S101ed1.CAT.SIGN. The signature file shall always be located in the same directory location as the S101ed1.CAT file.

The use of digital signatures shall be encoded:

Field name	***Comments***
S100_DatasetDiscoveryMetaData	
digitalSignatureReference: 1.0.0	Digital signature algorithm defined in S-100 part 15 ed 1.0.0
digitalSignatureValue: <value>	The digital signature for the file

The support files in the exchange set are encoded the same way in S-100SupportFileDiscoveryMetadata.