S-100Sec-4

Paper for Consideration by S-100 Encryption/Authentication Meeting / S-101 PT

S-100 Metadata – Algorithms

Submitted by:	S-100WG Chair; RMM; EM
Executive Summary:	S-100 metadata includes provisions for indicating encryption, signature, and compression/archive algorithms, but the actual algorithms have not been identified.,
Related Documents:	S-100 Eds. 3.0.0 and 4.0.0 (draft)
Related Projects:	--

Introduction / Background

Within the redline of S-100 Part 4a for edition 4.0.0 there is provision for S-100-based metadata to indicate the algorithms for encryption, signature, and compression by picking from enumerated lists. However, the actual algorithms have not been identified. This paper requests assistance with identifying the algorithms, especially for encryption and signature.

Given that the S-101 PT plans to work on an S-101 Data Encryption and Authentication Guide, the assistance of the S-101 PT and/or the S-100 Encryption/Authentication meeting is requested.

Analysis/Discussion

S100 WG2 made the following decisions:

> *3. Modify S-100 3.0 Part 4a S100_DatasetDiscoveryMetaData:digitalSignatureReference to have a value from a digitalSignature class, similar to S100_DataFormat: This was agreed and will be done as part of the metadata review.*
>
> *4. Modify S-100 3.0 Part 4a S100_ExchangeCatalogue:algorithmMethod to have a value from a compressionAlgorithm class, similar to S100_DataFormat: This was agreed and will be done as part of the metadata review.*
>
> *5. Modify S-100 3.0 Part 4a S100_DatasetDiscoveryMetaData:protectionScheme to have a value from an encryptionAlgorithm class, or specify the allowed algorithm values in the "Remarks" column: This was agreed and will be done as part of the metadata review (**Action 11**).*

The list of protection schemes in the S-100 metadata model currently includes only “S-63” as a placeholder. It does not include any signature algorithms. The only compression methods that have been considered so far are ZIP and RAR. It has been pointed out that ZIP and RAR are archive formats rather than compression algorithms.

Input is requested on:

1) Specification of the list of allowable signature algorithms including their designations, definitions, and specification of any parameters or versions (S100_DigitalSignatureAlgorithm literals).
2) Specification of the list of allowable protection schemes including their designations, definitions, and specification of any parameters or versions (S100_DigitalSignatureAlgorithm literals).
3) Specification of allowable archive formats including their designations, definitions, and specification of any parameters or versions (i.e., defining a new enumeration S100_AlgorithmMethod or

S100_ArchiveFormat) which can be used to make S100_ExchangeCatalogue.algorithmMethod an enumeration.

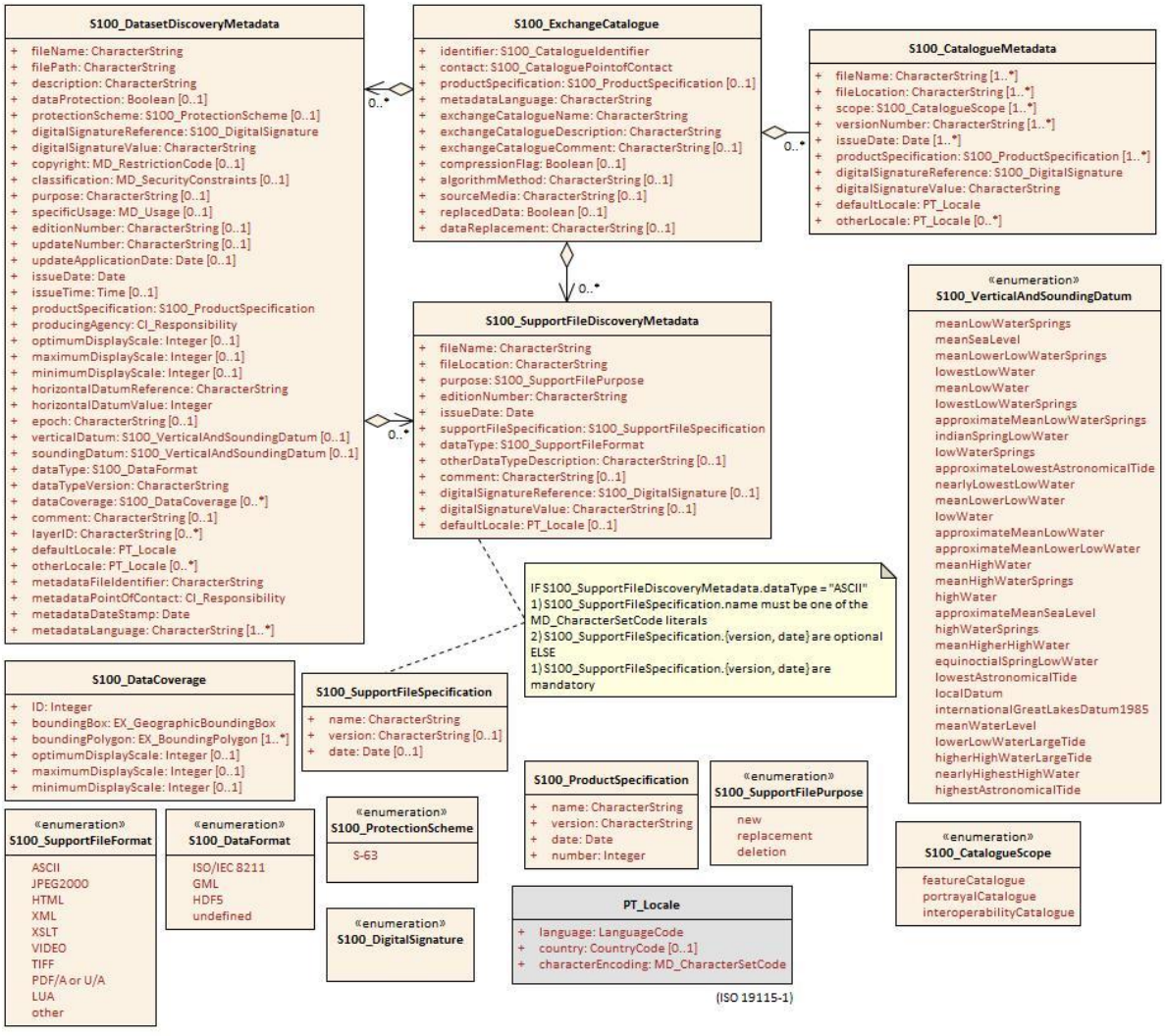
4) Consideration of any interactions between the relevant algorithms and methods is also requested. For example, since implementations of archive formats usually include choices between different methods of compression, the allowable compression schemes in the archive formats should also be considered

5) The utility (positive or negative) of adding 'undefined' values to each enumeration (to be interpreted as allowing the product specification to specify the algorithm).

6) Class, enumeration, and attribute names for the relevant items, as currently defined and as may be recommended in response to this paper.

Current model

The current state of the metadata model for S-100 Edition 4.0 (in preparation) is depicted in the figure that follows. The specific items relevant to this paper are defined in the tables following the figure.



The relevant definitions from S-100 Part 4a are in the tables that follow:

Attribute	compressionFlag	Is the data compressed	0..1	Boolean	Yes or No
Attribute	algorithmMethod	Type of compression algorithm	0..1	CharacterString	For example. RAR or ZIP

Attribute	dataProtection	Indicates if the data is encrypted	0..1	Boolean	0 indicates an unencrypted dataset 1 indicates an encrypted dataset
Attribute	protectionScheme	Specification or method used for data protection	0..1	S100_ProtectionScheme	For example S-63
Attribute	digitalSignatureReference	Digital Signature of the file	1	S100_DigitalSignature	Specifies the algorithm used to compute digitalSignatureValue
Attribute	digitalSignatureValue	Value derived from the digital signature	1	CharacterString	The value resulting from application of digitalSignatureReference

S100_DigitalSignature

Role Name	Name	Description	Mult	Type	Remarks
Enumeration	S100_DigitalSignature	Algorithm used to compute the digital signature	-	-	-
Value	(TBD)		-	-	

S100_ProtectionScheme

Role Name	Name	Description	Mult	Type	Remarks
Enumeration	S100_ProtectionScheme	Data protection schemes	-	-	-
Value	S-63	IHO S-63	-	-	

Justification and Impacts

Finalization of the algorithms and methods is needed for more complete test-beds and giving predictability for implementations of S-100 and various product specifications.

Action Required

The S-100 Encryption/Authentication Meeting / S-101 PT are requested to:

a. Identify the allowable algorithms or methods for digital signature, protection scheme, compression, and archive format.

b. Suggest definitions for the algorithms and methods including any parameters or versions.

c. Consider the definitions of the metadata elements as included in the tables and recommend revisions as appropriate.