S100TSM9-4.16

Paper for Consideration by S100TSM9

Dataset Cancellations without datafiles

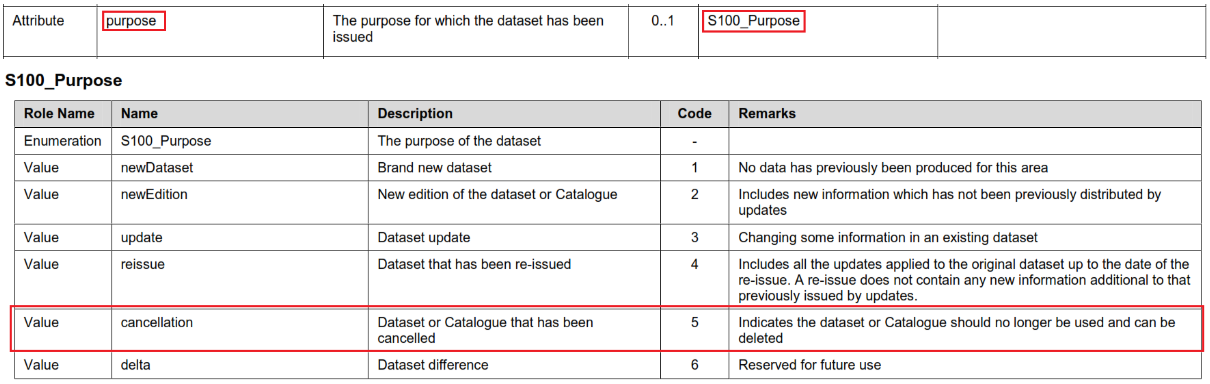
Submitted by:	PRIMAR
Executive Summary:	There are some issues identified regarding S-100 allowing cancellations to be issued as an instruction in the Exchange Catalogue metadata without an accompanying dataset file.
Related Documents:	S-100 5.0.0 Part 15 and Part 17
Related Projects:	

Introduction / Background

S-100 allows for cancellations to be issued as an instruction in the Exchange Catalogue metadata without an accompanying dataset file:

S-100 17-4.1 (text description below figure 17-2):
"…This level of flexibility is essential to properly support the mainstream use case of exchanging geospatial data, as well as the use cases for releasing dataset cancellation notices or new Catalogue releases without any data files present".

Technically this can be done by including the data file information in the exchange catalogue metadata and encode the DatasetDiscoveryMetadata attribute "purpose" (Type = S100_Purpose) with the value 5 (cancellation):



Attribute	purpose	The purpose for which the dataset has been issued	0..1	S100_Purpose	

S100_Purpose

Role Name	Name	Description	Code	Remarks
Enumeration	S100_Purpose	The purpose of the dataset	-	
Value	newDataset	Brand new dataset	1	No data has previously been produced for this area
Value	newEdition	New edition of the dataset or Catalogue	2	Includes new information which has not been previously distributed by updates
Value	update	Dataset update	3	Changing some information in an existing dataset
Value	reissue	Dataset that has been re-issued	4	Includes all the updates applied to the original dataset up to the date of the re-issue. A re-issue does not contain any new information additional to that previously issued by updates.
Value	cancellation	Dataset or Catalogue that has been cancelled	5	Indicates the dataset or Catalogue should no longer be used and can be deleted
Value	delta	Dataset difference	6	Reserved for future use

A couple of issues that should be resolved has been identified:

A: A fileless cancellation instruction as described above is not supported by the digital signature mechanism in S-100 Part 15.

B: The cancellation will not be part of a data file life cycle as is the case for the current S-57 ENCs.

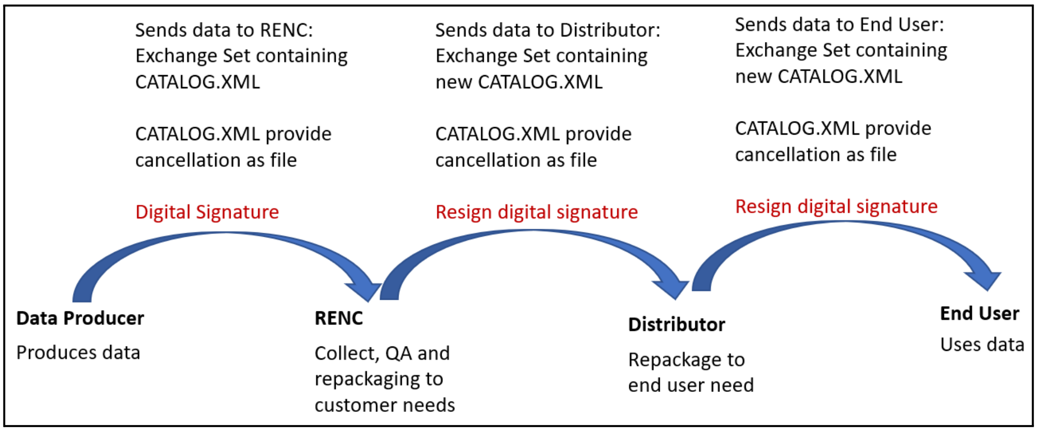
Analysis/Discussion

A:
S-100 part 15 defines a mechanism for digitally signing all the files included in an exchange set including the catalogue file. This mechanism applies to both dataset and support files. It is envisaged that some data producers will always digitally sign the datasets produced by them, supporting the possibility to trace the dataset all the way back to its origins. A RENC/service provider will/can co-sign such datasets.

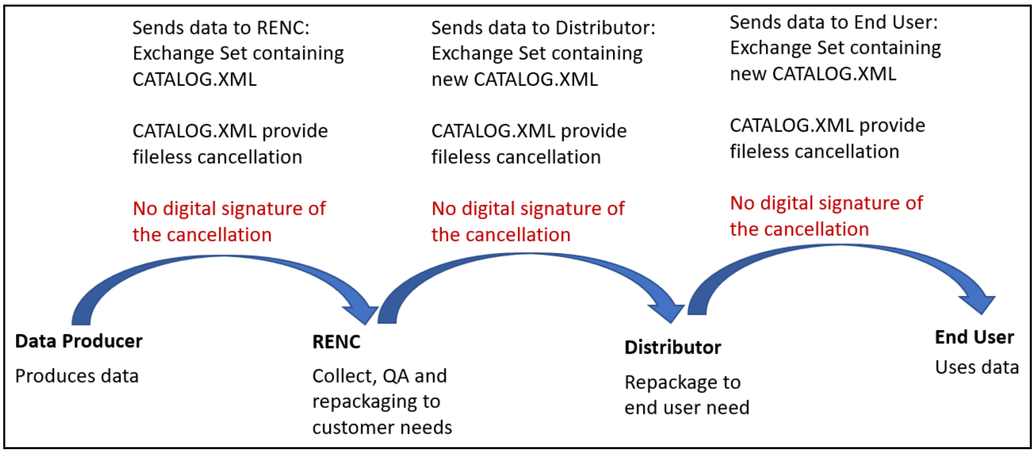
If a cancellation transaction is issued without an accompanying dataset file (fileless cancellation), S-100 requires that all the cancellation information must be encoded in the CATALOG.XML metadata. It will be the responsibility of the data recipient to create the required transaction information for the internal database operation.

It will be possible for the data producer to digitally sign the CATALOG.XML and all dataset/support files before providing them to a RENC/service provider. A RENC/service provider will authenticate the received signature before any processing of the received exchange set. A RENC/Distributor will always create new exchange sets before distribution when it is packaging datasets from multiple providers and in accordance with end-user subscription. These exchange sets and corresponding CATALOG.XML file can never re-use any of the signature information applied by the data producer.

If,as is the current situation with S-57, the cancellation transaction is encoded in a separate cancellation update file, it will be possible for a data producer to digitally sign the update file. A RENC/distributor can resign the update file and the data recipient can trace the origins of the file back to the data producer. This process is illustrated in the following figure:



If however, a cancellation transaction is issued without an accompanying dataset file (fileless cancellation), there will be no digital signature available for the cancellation which can be resigned by the service provider. This process is illustrated in the following figure:



In this situation the only element containing the cancellation instruction is the CATALOG.XML. CATALOG.XML can be digitally signed by producer, by RENC and by Distributor, but as all these 3 instances creates new compositions of Exchange Catalogues to tailor individual needs, the signatures on the CATALOG.XML cannot be resigned further down the value chain. And as such the origin of the cancellation instruction is lost.

The consequence is that it will not be possible to trace the origins of a cancellation transaction back to the data producer since it will only contain the RENC/distributor digital signature. **This raises the question if this poses a security risk as it will then not be possible to verify the origin of the cancellation instruction**. In theory a RENC/Service Provider and Distributor could issue a cancellation instruction not being issued by a producing agency.

If the above scenario is considered as a security risk, to mitigate it a data producer digital signature shall follow a cancellation update all the way to the end-user. Then solutions must be established within the standard to support this requirement. Possible solutions can be:

- S-100 Part 15 must be extended to cater for the possibility to digitally sign the cancellation instruction within the DatasetDiscoveryMetadata.
- Special instructions must be defined for how a data producer shall create cancellation updates, how RENC/Distributors shall process cancellation updates, and how end-user systems shall process cancellation updates.

Another topic is whether fileless cancellation will be the only cancellation mechanism supported by S-100. If yes then this should be clearly stated, and further descriptive text on cancellation guidance should be provided in Part 17.

B:

From a service provider viewpoint a product (data file) has a life cycle. This starts with the initial version of a data file in edition 1, and ends with a cancellation update after 0-n editions (and 0-n updates/reissues between each edition if product specification supports the update structure).

If the fileless cancellation is to be used, the endpoint of a data file lifecycle will not be linked together with the data file itself (by issuing a cancellation update using edition nr 0 and update number as is currently done in S-57).

Many different systems are available to process exchange sets, both from a data producer and end-user perspective. Many of these systems have been developed to support S-57 exchange sets, and will later be upgraded to support S-100 products. Many of these systems have been designed around the product or data lifecycle concept established with S-57. We should carefully examine if this change in how the termination in a product life cycle is encoded and the impact on user systems. The end-user systems can no longer rely on there always being an update file available to support every update transaction, and it will require that the end-user system must create and record their own database update transaction. This is to make sure that the file-less cancellation events are properly versioned and released in the same way as other data set version events.

It has also been easy for a RENC/distributor to create on the fly custom made exchange sets for an end-user - package all the relevant data/support files and create the corresponding CATALOG.XML file. In a fileless solution this task will be more complicated depending on if aggregated or delta update exchange sets are to be created. It might be necessary to explicitly state how end-user systems, for type approval purposes, shall perform if updates are not processed sequentially, and a cancellation message is not received.

To avoid this, it would be helpful if the exchange catalogue metadata could also include an entry for the data file adjusting update number accordingly (even though the data file itself is not present in the exchange set).

Conclusions

- It must be agreed upon if missing digital signing of the cancellation instruction poses a security risk, and if yes a solution must be provided.
- If S-100 supports both options (fileless cancellation and cancellation using a data file) must be determined. Further descriptive text on cancellation guidance should be provided in Part 17.
- Consider if a fileless cancellation still could lead to an uptick in update number of the data file information in the Exchange Catalogue metadata (CATALOG.XML).
- Explanatory text for cancellation handling must be added in S-100 Part 17.

Action Required of S100TSM

The S100TSM is invited to:
Note the paper and discuss proposed changes.