S-104/S-111PT

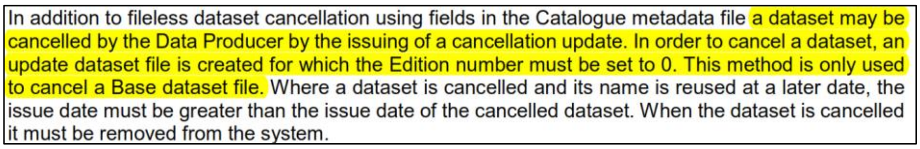
Paper for Consideration by S-104/S-111PT

Cancellation support clarification

Submitted by:	PRIMAR
Executive Summary:	S-100 supports 2 mechanisms for cancellations of datasets. Currently cancellation implementation in S-104 and S-111 is marked as informative, now is the time to further describe the cancellation mechanism to be supported. Of the 2 cancellation mechanisms S-104 and S-111 seems to be supportive of the fileless mechanism. There is an identified security breach with the fileless cancellation mechanism that must be taken into consideration before making a decision on how cancellations should work in S-104 and S-111.
Related Documents:	S-100 5.1.0 Part 17 S-104 1.1.0 S-111 1.2.0 WENDWG14 paper: Severity of cancellation traceability
Related Projects:	

Introduction / Background

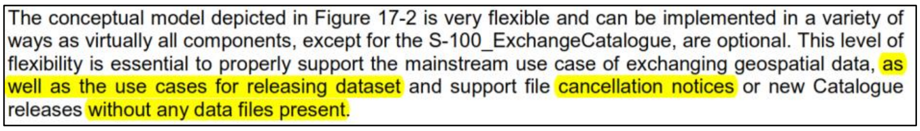
In S-100 there are two mechanisms defined for cancelling datasets. The “traditional” mechanism is well known from S-57, where a cancellation is issued as an update of the dataset. This update is issued as a dataset file. When loaded into the end user system the update dataset encoding tells the system that the base dataset is to be cancelled, and as a consequence the cancelled dataset is removed. S-100 describes this file-based cancellation in chapter 17-4.4.1:



In addition to fileless dataset cancellation using fields in the Catalogue metadata file a dataset may be cancelled by the Data Producer by the issuing of a cancellation update. In order to cancel a dataset, an update dataset file is created for which the Edition number must be set to 0. This method is only used to cancel a Base dataset file. Where a dataset is cancelled and its name is reused at a later date, the issue date must be greater than the issue date of the cancelled dataset. When the dataset is cancelled it must be removed from the system.

In S-100 it is expected that the end user system will find the information needed in CATALOG.XML, which can be seen as the entry point for all information packaged in an S-100 defined exchange set. For the above-described file-based cancellation mechanism, this means that the cancellation dataset will be packaged in the exchange set, and CATALOG.XML contains additional discovery metadata describing that this is a cancellation.

This ability to encode cancellation instruction as part of the CATALOG.XML dataset discovery metadata opens the door for the second cancellation mechanism defined by S-100, the fileless cancellation. This is briefly described in S-100 17-4.1 (text description below figure 17-2):



The conceptual model depicted in Figure 17-2 is very flexible and can be implemented in a variety of ways as virtually all components, except for the S-100_ExchangeCatalogue, are optional. 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 and support file cancellation notices or new Catalogue releases without any data files present.

Analysis/Discussion

For implementers of S-100 and the various product specifications, it is essential to know which of the cancellation mechanisms the product specification supports, or if it supports both.

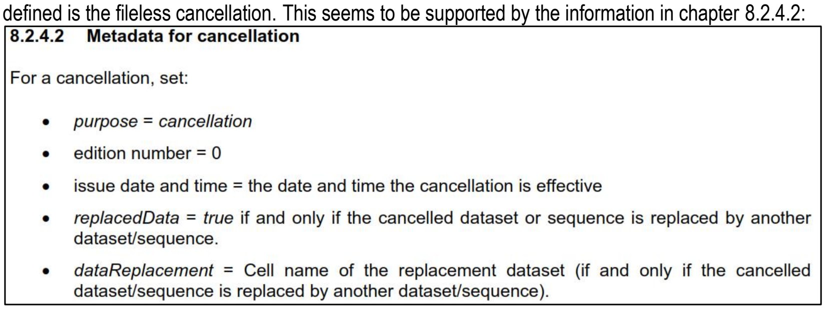
As long as the product specification does not restrict itself to one solution, the anticipation would be that both are supported.

Section 8.2 in S-104/S-111 defines the cancellation information to be informative:

8.2 General principles for dataset maintenance especially cancellation are being developed in the S-100 Working Group and this section is therefore marked Informative in this edition of S-104.

8.2 General principles for dataset maintenance especially cancellation are being developed in the S-100 Working Group and this section is therefore marked Informative in this edition of S-111.

As long as S-104/S-111 doesn't support update dataset files, the only cancellation mechanism that can be defined is the fileless cancellation. This seems to be supported by the information in chapter 8.2.4.2:



8.2.4.2 Metadata for cancellation

For a cancellation, set:

- *purpose* = *cancellation*
- edition number = 0
- issue date and time = the date and time the cancellation is effective
- *replacedData* = *true* if and only if the cancelled dataset or sequence is replaced by another dataset/sequence.
- *dataReplacement* = Cell name of the replacement dataset (if and only if the cancelled dataset/sequence is replaced by another dataset/sequence).

There probably should be some kind of statement in the Product Specifications clearly expressing that fileless cancellation mechanism is the only one supported, to avoid confusion on the topic.

However, there is an unresolved issue with fileless cancellations it is important to be aware of before making a decision. Currently there is no way to create digital signatures for those types of cancellations, and this may be considered to be a significant breach of the security scheme. WENDWG14 will be discussing this in their February 2023 meeting. The document to be discussed is available in Annex A for S-104/S-111PTs convenience.

If the project team, due to the identified security breach issue, should decide to not support the fileless cancellation mechanism, the solution would be to add update as a type of dataset file and at the same time clearly state that fileless cancellation mechanism is not supported. (For inclusion of update as type of dataset file, refer to S-101 1.2.0 where this is clearly defined).

Conclusions

- S-104/S-111 seems to be supporting the fileless cancellation mechanism only.
- There is an identified security breach with the fileless cancellation mechanism that must be taken into consideration before making a decision on how cancellations should work in S-104/S-111.
- If the identified security breach is considered too severe, S-104/S-111PT must consider implementing support for update dataset files to support the file-based cancellation mechanism.
- Either preferred way forward would require clarification to the product specification to clearly define which cancellation mechanism that is/and is not supported.

Action Required of S-104/S-111PT

The S-104/S-111PT is invited to:

- Note the paper and discuss the severity of security breach in the fileless cancellation mechanism.
    - Take into consideration the WENDWG discussion on the topic.
- Discuss and decide how to implement valid support for cancellations, either by using the file-based cancellation mechanism, or by using the fileless cancellation mechanism, or by using both.

- Take any action appropriate.

Annex A

WENDWG14

Paper for Consideration by WENDWG14

Severity of cancellation traceability

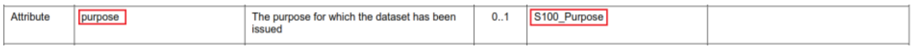
Submitted by:	PRIMAR/S-100WG Chair
Executive Summary:	At the S-100 Test Strategy Meeting in 2023 (TSM9) an issue related to the S-100 provision of a fileless cancellation mechanism was raised by PRIMAR. A consequence of using the mechanism is the inability to verify the origin of a cancellation instruction. TSM9 approved an action to approach WENDWG for further guidance related to the severity of cancellation traceability.
Related Documents:	S-100 5.1.0 Part 15 and Part 17 S100TSM9-4.16_2023_EN_Dataset Cancellations without datafiles
Related Projects:	

Introduction / Background
The following action came out from the 9th S-100 Test Strategy Meeting in 2023:
[Action 9/22] S-100WG Chair (supported by PRIMAR) to approach WENDWG to discuss severity of cancellation traceability.

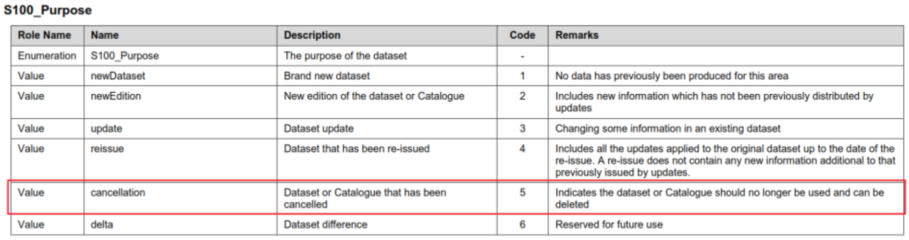
S-100 allows for cancellations to be issued as an instruction in the Exchange Catalogue metadata without an accompanying dataset file:

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

The following issue has been identified and should be further discussed by the WENDWG:
A fileless cancellation instruction as described above is not supported by the digital signature mechanism in S-100 Part 15.

The consequence is inability of tracing the cancellation back to the issuing authority, at least at the same level of traceability that is possible for file-based cancellations.

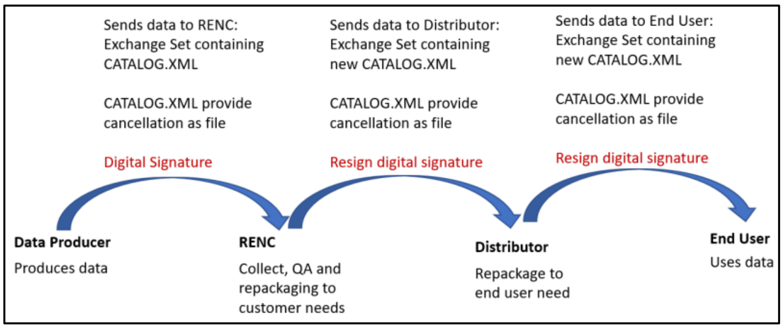
WENDWG is invited to discuss if the digital signature of the exchange catalogue itself offers a good enough level of security for fileless cancellations, or if S-100WG should investigate further to find a better solution.

Analysis/Discussion
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.

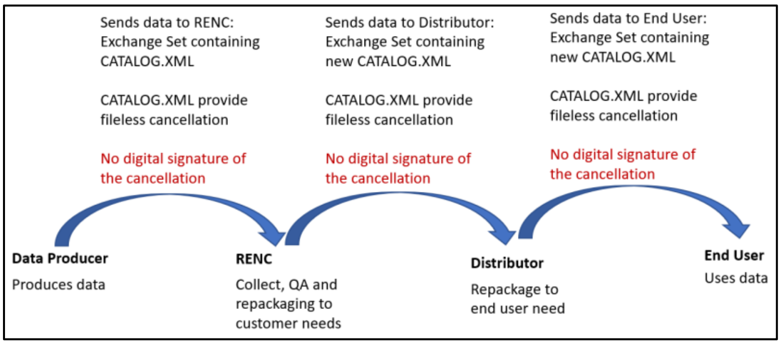
If a cancellation transaction is issued without an accompanying dataset file (fileless cancellation), S-100 requires that all the cancellation information must be encoded in the CATALOG.XML metadata. It will be the responsibility of the data recipient to create the required transaction information for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


Sends data to RENC:
Exchange Set containing CATALOG.XML
CATALOG.XML provide fileless cancellation
No digital signature of the cancellation
Sends data to Distributor:
Exchange Set containing new CATALOG.XML
CATALOG.XML provide fileless cancellation
No digital signature of the cancellation
Sends data to End User:
Exchange Set containing new CATALOG.XML
CATALOG.XML provide fileless cancellation
No digital signature of the cancellation
Data Producer
Produces data
RENC
Collect, QA and repackaging to customer needs
Distributor
Repackage to end user need
End User
Uses data

In this situation the only element containing the cancellation instruction is 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.

Conclusions

- It must be agreed upon if missing digital signing of the cancellation instruction poses a security risk. If yes actions to find a solution should be taken.
- Further descriptive text on cancellation guidance should probably be provided in Part 17.
- Explanatory text for cancellation handling should be added in S-100 Part 17.

Commented [SS1]: Perhaps a string could be included in CATALOG.XML that could be digitally signed?
E.g., "dataSetId:cancel"

Action Required of WENDWG

The WENDWG is invited to:

- Note the paper and discuss the severity of missing digital signatures for fileless cancellations.

Take any action appropriate.