WENDWG14-07.1G

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.

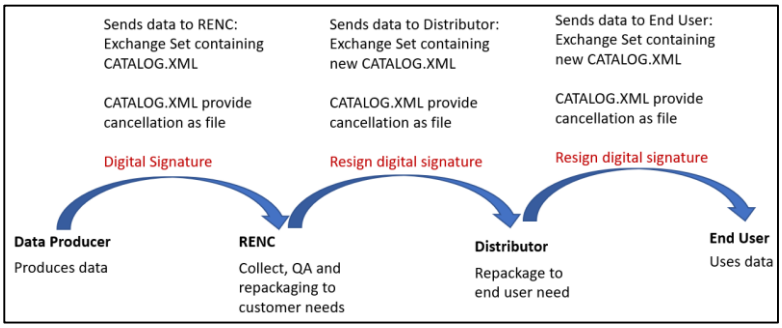
Analysis/Discussion

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.

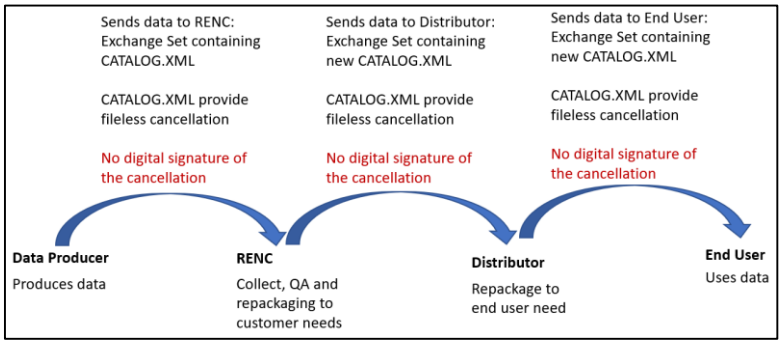
If a cancellation transaction is issued without an accompanying dataset file (fileless cancellation), S-100 requires that all the cancellation information must be encoded in the CATALOG.XML metadata. It will be the responsibility of the data recipient to create the required transaction information for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



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.

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.

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