NOKIA

Evaluation for KI#5 (ML model sharing)

eNA_Ph3 Conf Call

SA2#152e

29 July 2022

Key principles

- The KI#5 aims at enabling the sharing of an ML model between AnLF and MTLF possibly from different vendors
  - The KI#5 does not preclude the scenario in which the ML model is transferred between the two
- Running a model from another vendor shall be regulated by preliminary agreements
  - Including business agreements
- ML model sharing shall be possible without disclosing intellectual property and other secret information

KI#5: overview of solutions (1/2)

Sol #	Title	Source	Main principles	Evaluation
13	NWDAF MTLF and NWDAF AnLF interoperability support for registration and discovery in 5GC	**Intel**	An NWDAF containing MTLF shall include **ML model file serialization format** supported in the ML model filter information for the trained ML model per Analytics ID(s).	How ML model privacy is supported when NWDAF containing MTLF and NWDAF containing AnLF belong to different vendors is in scope of SA WG3. The common file format between ANLF & MTLF is not sufficient for the model to be interoperable
14	Enhance trained ML Model sharing via ML Model format	**Vivo**	An NWDAF containing MTLF shall include Supported **ML model format information** and **Supported AI Framework Information** in the ML model filter information for the trained ML model per Analytics ID(s). Proposal to use ONNX to share ML models	Share common aspect with solution 13 ONNX is only for neural networks The model metadata is not defined as part of this solution.
15	ML model sharing with different AnLF providers	**Docomo**	MTLF includes the support of **interoperable indicator which encodes e.g. the 3GPP-specific Vendor Id** in the NF profile for the NRF registration, and the consumer (AnLF) discovery and select the MTLF that interoperability for an analytic ID.	The solution attempts to resolve the “ML model privacy” issue
47	Sharing models between NWDAFs	**Ericsson**	Pre-condition to share models: business aspects are in place and interoperability tests are done. Then an **Interoperable Token** is known by both MTLF and AnLF and the token registered at NRF. ML models to be shared as executable software such as **containers**	Most of the technical challenges are “resolved” by the precondition Does a container comply with the current format of an ML model, i.e., “file”?

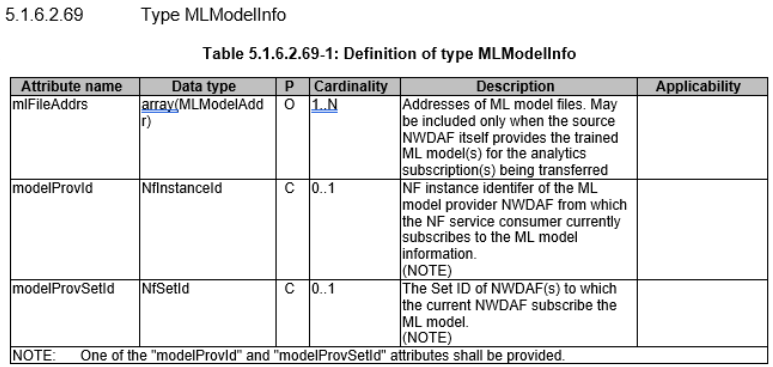
KI#5: overview of solutions (2/2)

- Solutions #13 and #14 propose to introduce descriptors of the ML model artifact,
  - This enables interoperability based on the support of the source and target NFs to the capabilities and requirements contained in such descriptors

- Solutions #15 and #47 propose to use an interoperability indicator/token
  - Sol. #15 limits the scope of the indicator to capture the agreements among vendors.
  - In Sol. #47, the token is also a guarantee that preliminary interop tests are conducted

Open questions (1/2)

- What is an ML model? There is **no definition** available
- What is the format of the ML model?
  - Rel. 17 specifies MLModelInfo data structure in TS 29.520
  - Essentially it is a file referred by its URL



5.1.6.2.69 Type MLModelInfo

Table 5.1.6.2.69-1: Definition of type MLModelInfo

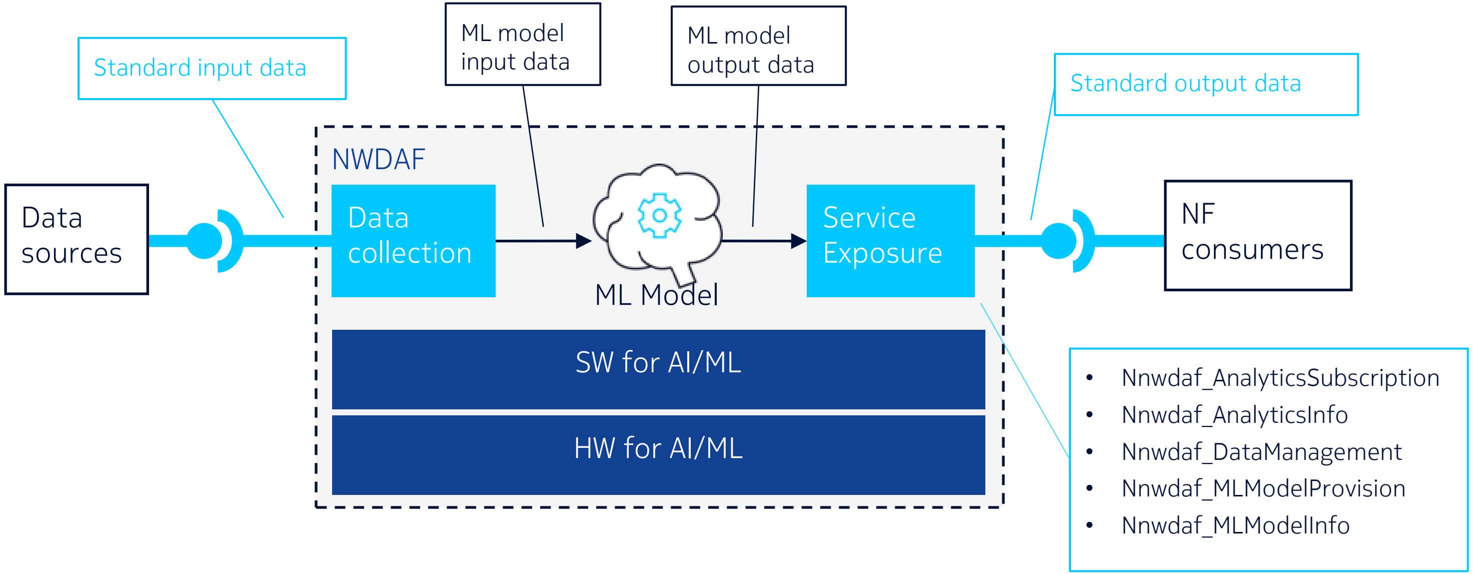
Attribute name	Data type	P	Cardinality	Description	Applicability
mlFileAddrs	array(MLModelAddr)	O	1..N	Addresses of ML model files. May be included only when the source NWDAF itself provides the trained ML model(s) for the analytics subscription(s) being transferred	
modelProvId	NfInstanceId	C	0..1	NF instance identifer of the ML model provider NWDAF from which the NF service consumer currently subscribes to the ML model information. (NOTE)	
modelProvSetId	NfSetId	C	0..1	The Set ID of NWDAF(s) to which the current NWDAF subscribe the ML model. (NOTE)	

NOTE: One of the "modelProvId" and "modelProvSetId" attributes shall be provided.

- What is the software support?
  - ML-specific interexchange formats written in descriptive language, e.g., ONNX, vs executable software, e.g., container
- Who does the ML model belong to?
  - In certain scenarios it might not belong to the NWDAF vendor

Open question 2/2

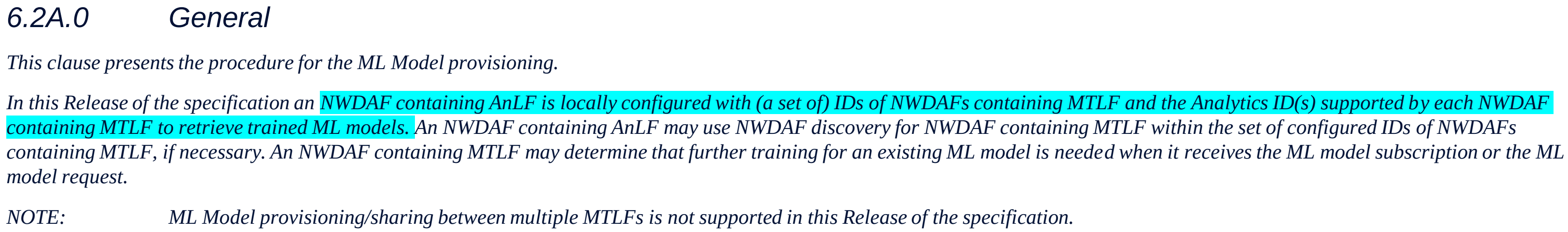
- □ To ensure interoperability, the input and output data of an ML model shall be known
  - □ **None** of the solutions documented so far address this problem



- Nnwdaf_AnalyticsSubscription
- Nnwdaf_AnalyticsInfo
- Nnwdaf_DataManagement
- Nnwdaf_MLModelProvision
- Nnwdaf_MLModelInfo

Observation and conclusion

- Currently, in Rel. 17 TS 23.288, ML model sharing is enabled on AnLF and MTLF by configuration



6.2A.0 General

This clause presents the procedure for the ML Model provisioning.

In this Release of the specification an NWDAF containing AnLF is locally configured with (a set of) IDs of NWDAFs containing MTLF and the Analytics ID(s) supported by each NWDAF containing MTLF to retrieve trained ML models. An NWDAF containing AnLF may use NWDAF discovery for NWDAF containing MTLF within the set of configured IDs of NWDAFs containing MTLF, if necessary. An NWDAF containing MTLF may determine that further training for an existing ML model is needed when it receives the ML model subscription or the ML model request.

NOTE: ML Model provisioning/sharing between multiple MTLFs is not supported in this Release of the specification.

- The use of interoperability indicators/tokens is only a bit more flexible, because it shifts the problem to configure such tokens
- The use of descriptors would enable more flexible and dynamic operations, but the current solutions only address a small aspect

<u>CONCLUSION</u>

- No solution documented so far fulfills the objective of KI#5, so no solution can be recommended as baseline for normative work

NOKIA