Modelica Change Proposal MCP-0039  
SEMLA (Standardized Encryption of Modelica Libraries and Artifacts)  
Jesper Mattsson, Iakov Nashimovski, Hubertus Tummescheit  
Status: In Development  
2021-04-09 version v1

**Summary**

This specification describes a container for distributing Modelica libraries and a protocol for how a Modelica tool should communicate with an executable for licensing and decryption of the library. The following scenarios are supported:

* Both code encryption and licensing are supplied by library vendor.
* Licensing is handled through a Modelica tool’s licensing mechanism, and code encryption is supplied by library vendor.
* Library is open-source, no encryption or licensing is used.

The executable for licensing and decryption of the library is supplied by the library vendor and will hereafter be referred to as the “LVE” (Library Vendor Executable). The LVE should handle decryption and may optionally handle licensing. The LVE is packaged together with the library in a container. Several LVE may be included in the container for different platforms.

**Revisions**

|  |  |
| --- | --- |
| *Date* | *Short description of revision* |
|  |  |
| April 9, 2021 | 1st MCP version converted from Modelon internal documentation to MCP format |

**Contributor License Agreement**

All authors of this MCP or their organizations have signed the “Modelica Contributor License Agreement”

Table of Contents

[1. Rationale 2](#_Toc68876083)

[1.1 Use cases 2](#_Toc68876084)

[2. Proposed Changes in Specification 2](#_Toc68876085)

[3. Backwards Compatibility 2](#_Toc68876086)

[4. Tool Implementation 2](#_Toc68876087)

[4.1 Experience with Prototype 3](#_Toc68876088)

[4.2 Required Patents 3](#_Toc68876089)

[5. References 3](#_Toc68876090)

[Appendix A First Appendix 4](#_Toc68876091)

# Rationale

With a broad ecosystem of Modelica tool and library vendors now active, a simplified sharing of libraries between different tools, as well as of private models and libraries between collaborators in Model Based Design will increase the attractiveness of Modelica as a preferred solution for model based systems engineering and design. A format as proposed would allow to independent developers to develop libraries in a single format that can be loaded and processed by all compliant Modelica tools, as well as monetization of such libraries.

The proposal describes a container format for Modelica Libraries that can be both encrypted and unencrypted. It also describes an executable called the “LVE” that does the decryption of a library as well as the (optional) licensing. The proposal also describes a communication protocol between the LVE and a Modelica tool that would like to read an encrypted and (optionally) licensed library. This setup allows to use both a licensing mechanism provided by the library vendor (through the LVE), and a mechanism that is specific and proprietary to a Modelica tool, and only the encryption is handled through the LVE. Note that licensing through the Library vendor is a critical component in allowing independent Library developers to enter the market for Modelica Libraries.

Note that the proposal tries to reuse known and well-tested open-source technologies – like openssl – as much as possible to reduce risk and implementation.

## Use cases

* Use case 1: An independent Library Vendor would like to provide a single, unified library distribution to several Modelica tools. A single container file can be distributed to end users of different tools, and the packaging and distribution effort for library developers is reduced.
* Use case 2: A supplier and an OEM want to share models that contain sensitive IP. Licensing is not necessary, but it is possible to share encrypted models between them. Note that SEMLA only takes care of the storage format of the models on disk, the protection inside the tool continues to be the responsibility of the tool that loads the model.
* Use case 3: A Modelica end user company wants to use 1 commercial Modelica Library with different Modelica tools. In the current setup, the end user might have to pay each tool vendor separately for the same library. SEMLA and licensing by the Library vendor allows end users to use a single license for a library in multiple tools.

# Proposed Changes in Specification

The precise text of the proposed changes with respect to Modelica Specification 3.3 are in the accompanying document MCP\_00XX\_SEMLA\_v1\_SpecChanges.docx.

# Backwards Compatibility

This MCP is orthogonal to any previous parts in the specification and does not require any considerations w.r.t backwards compatibility. Note that this proposal is orthogonal to and does not require any changes to the protection annotation in the Modelica Language Specification.

# Tool Implementation

An open source reference implementation is available at <https://github.com/modelon-community/SEMLA>. Is is licensed under the BSD 3-clause license by Modelon and available for reuse or modification by any interested party. This prototype has been in use since 2015 by Modelon, as well as by ANSYS as a licensor of Modelon’s Modelica compiler. Recently, OpenModelica has also implemented support that has been tested by Modelon to also work well with Modelon’s commercial libraries.

## Experience with Prototype

The protpype referenced above has been in use since 2015 and has generally been positive and without problems. There are now two independent implementations om

## Required Patents

At best of your knowledge state any patents that would be required for implementation of this proposal.

# References

1. <https://www.openssl.org/>
2. <https://github.com/modelon-community/SEMLA>
3. <https://openmodelica.org/doc/OpenModelicaUsersGuide/latest/encryption.html>
4. <https://www.modelon.com/leverage-standardized-encryption-and-licensing-for-modelica-libraries/>

First Appendix

All additional material is available in the referenced MCP\_00XX\_SEMLA\_v1\_SpecChanges.docx.