cosin
scientific software

FTire

Digital rights management for road surface models

Gerald Hofmann & Michael Gipser
cosin scientific software

Synopsis

Owners of high quality road data (licensors) wish to provide a copy of their intellectual property to users of their data in a secure way, that excludes unauthorized copying and sharing of the data by the end user.

The concept of digital rights management (DRM) for road data requires an encryption key exchange scheme for managing fine-grained user rights and policing the usage & scope of shared road data.

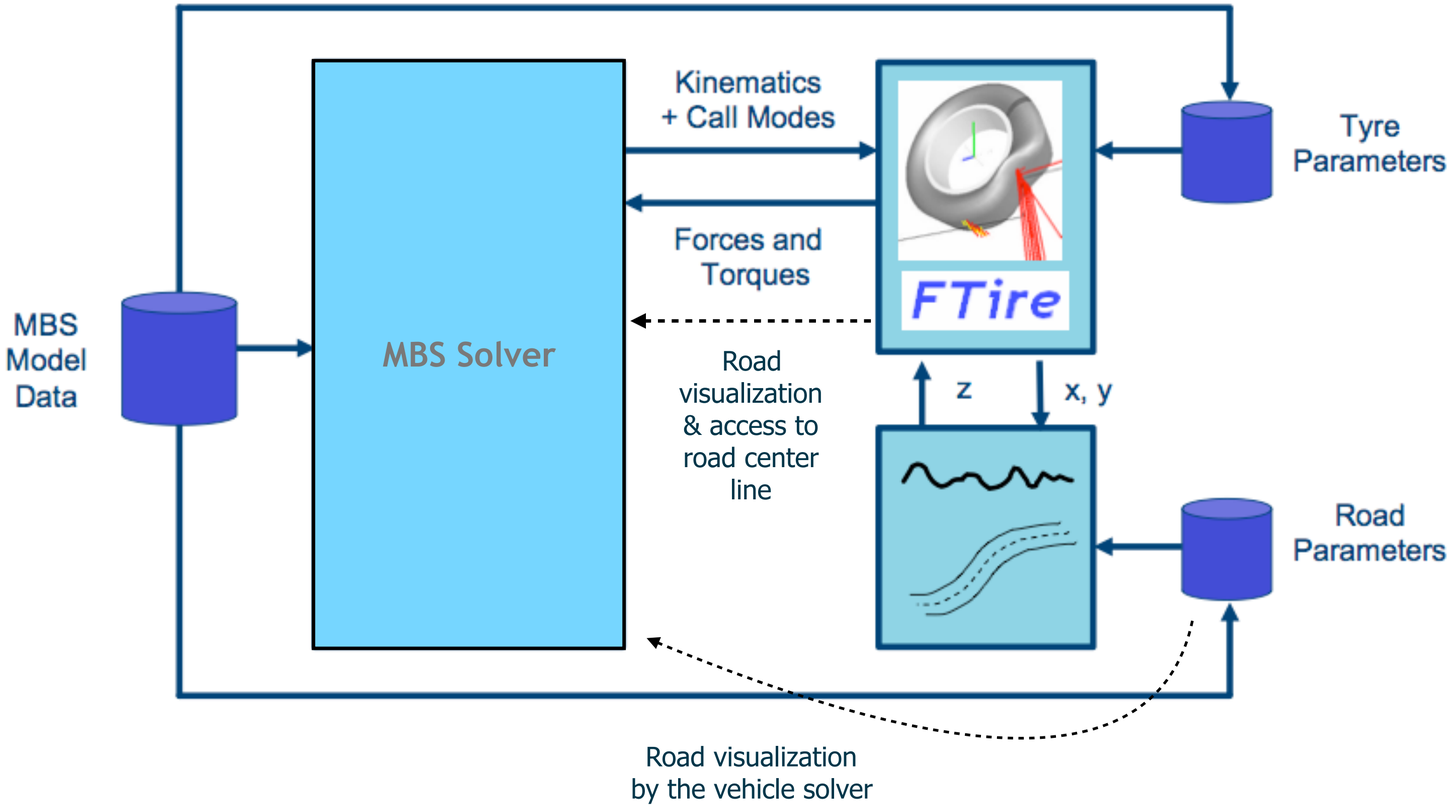
Synopsis

Applying DRM to digital road data makes possible an all new business case for providers and owners of high quality road data.

- Offer access to a road file database on a lease based business model („Digital road marketplace“)
- Limit usage to particular users or user groups, time period or even target systems (e.g. driving simulator or testbed system)
- Share proprietary road data with subcontractors on a „per project“ basis

Data providers and consumers

In vehicle dynamics simulation, the „consumer“ of the road data is the tire model in the first place.

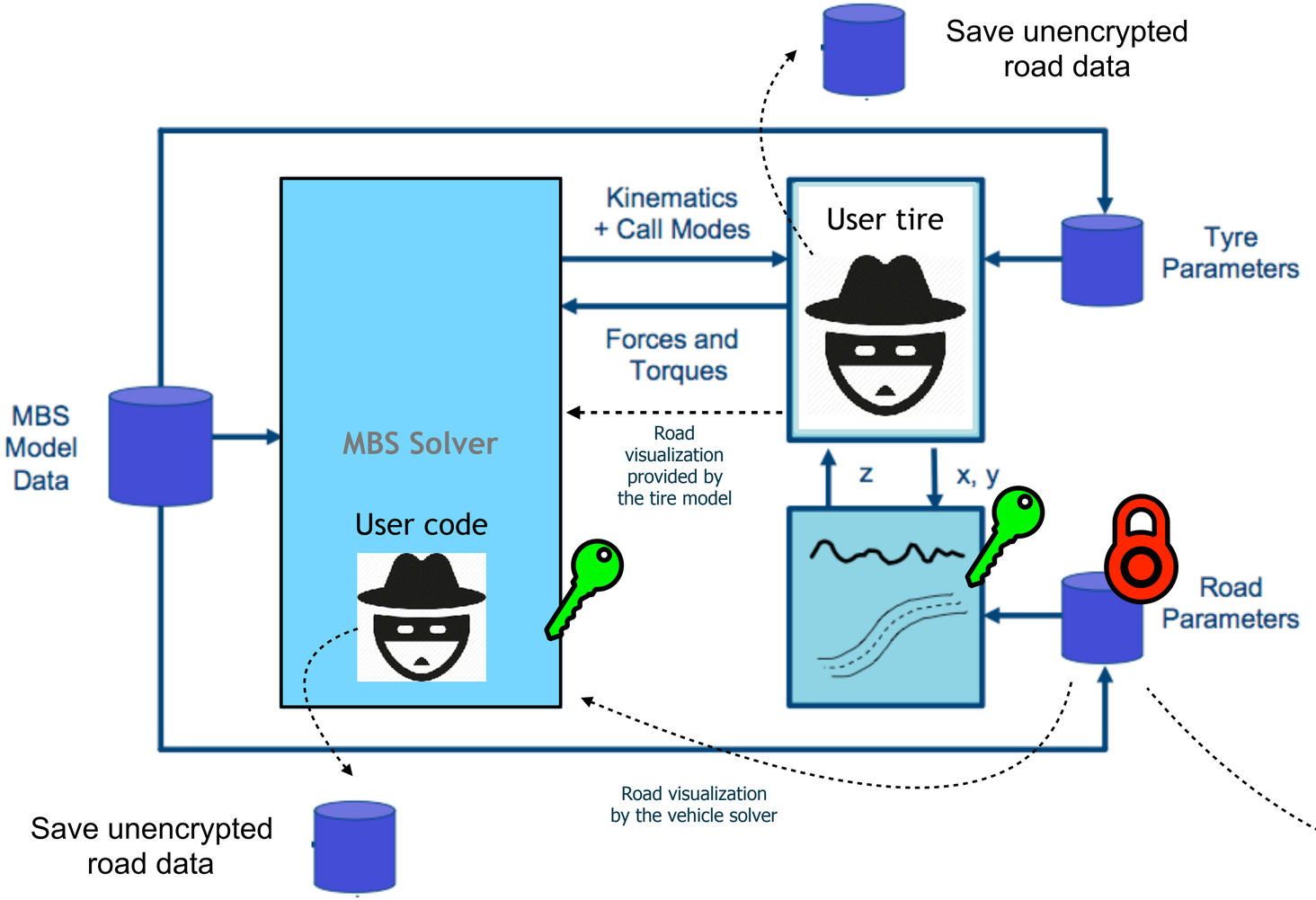


The vehicle solver optionally may want to access road data for visualization or as input to the driving controller system.

Access to the road can be done by loading the road data by the vehicle solver or by querying the road through the tire model.

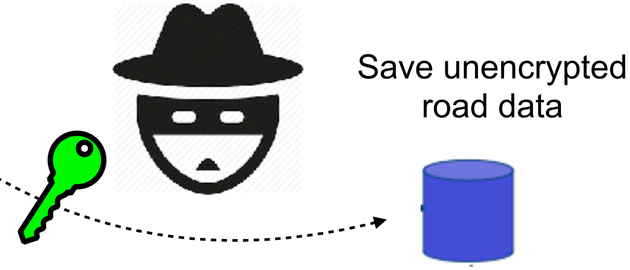
Password protected road data

Protecting the road data by a password seems to be a viable approach.



The password needs to be set by the licensor and needs to be shared with all „consumers“ to unlock the road data file.

The password is a shared secret and unauthorized dissemination can’t be prohibited by technical means.



Password protected road data

- Password needs to be shared with all „consumers“ and is not a reliable „secret“.
- Unlocking road data by password does not prohibit saving of the decrypted data by „rogue“ user code even from inside an authorized context (vehicle simulation) and even if the password is hidden from the end user by a pre-configured vehicle solver.
  E.g. user written code that pretends to be a tire model or visualization plugin, but actually writing out clear text road data.
- Disclosed passwords are not revocable, do not expire and can be used multiple times concurrently.

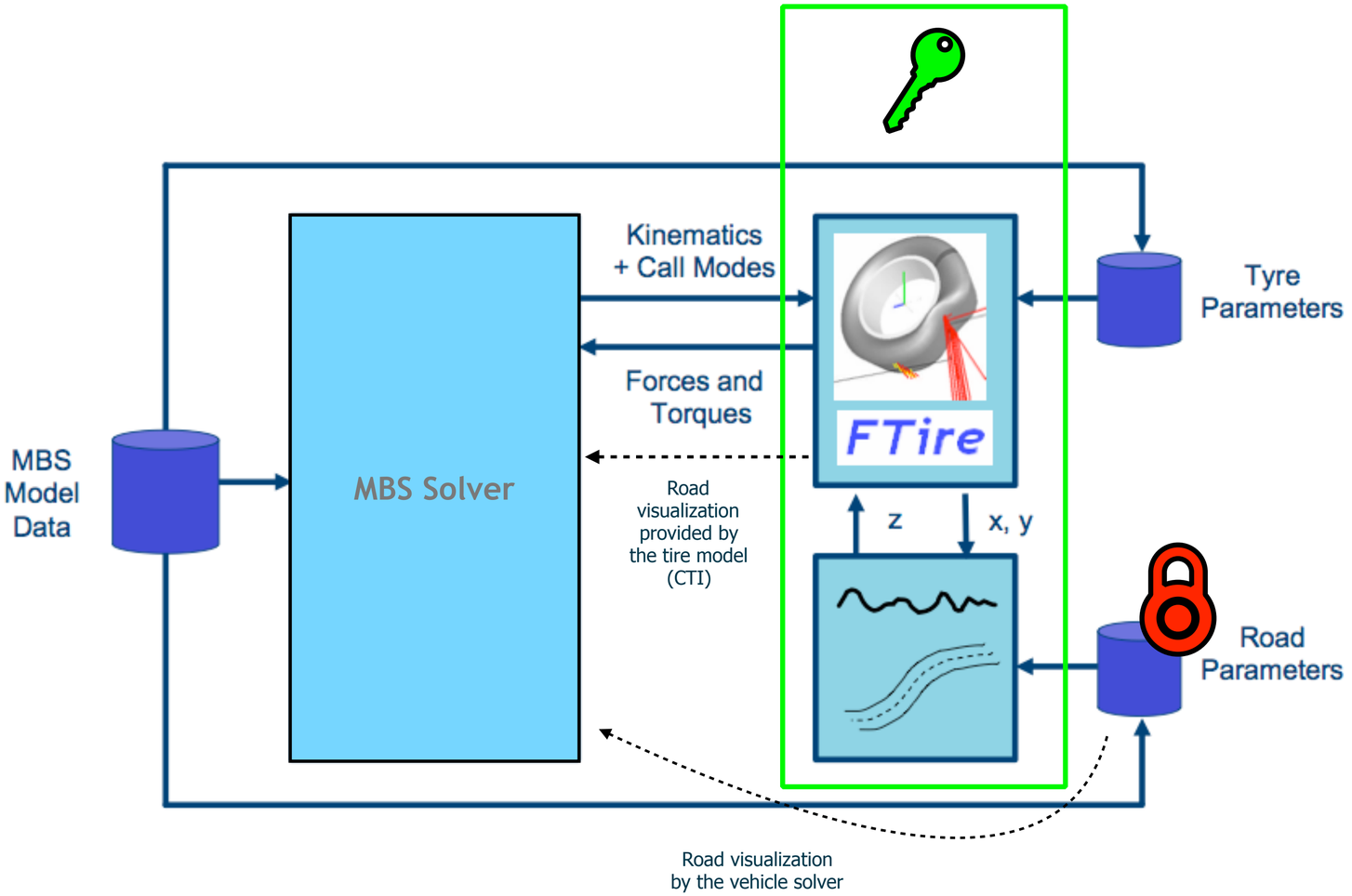
Generally: Protecting shared data by a password is useless…

Encryption is only a technical means to establish DRM, but not a solution by itself. Passwords are unsuitable to accomplish the requirements of a road data DRM system.

A trusted environment with a key exchange infrastructure is essential.

FTire as a trusted environment

The decryption key must only be shared with a trusted environment, provided by CTI.



How can the licensor deploy the decryption key without sharing a secret with the end user?

How to deal with consumers outside the trusted environment?

De-/Encryption key infrastructure

The licensing system can be used to act as a key management system.

The decryption key is **derived** from the name tag after the respective license has been confirmed

Trusted environment confirms/locks the license for a particular road data file tag

License key:
Nuerburgring_HighRes

- License expiration
- License count
- Target system
- Licensed end user

OLicense

Kinematics + Call Modes

Forces and Torques

Tyre Parameters

MBS Model Data

MBS So

FTire

FTire/core solver license

Low resolution visualization provided by the trusted environment (CTI)

z

x, y

Nuerburgring_HighRes

Parameters

cosin/tools **derives** an encryption key from the name tag and creates an encrypted road data file. The actual encryption key used is not known to or set by the provider.

No way back at this point. Even cosin/tools can't decrypt the road data.

cosin/tools

Nuerburgring_HighRes

Assigned name tag:
Nuerburgring_HighRes

Consumers outside the trusted environment have no access to the decryption key

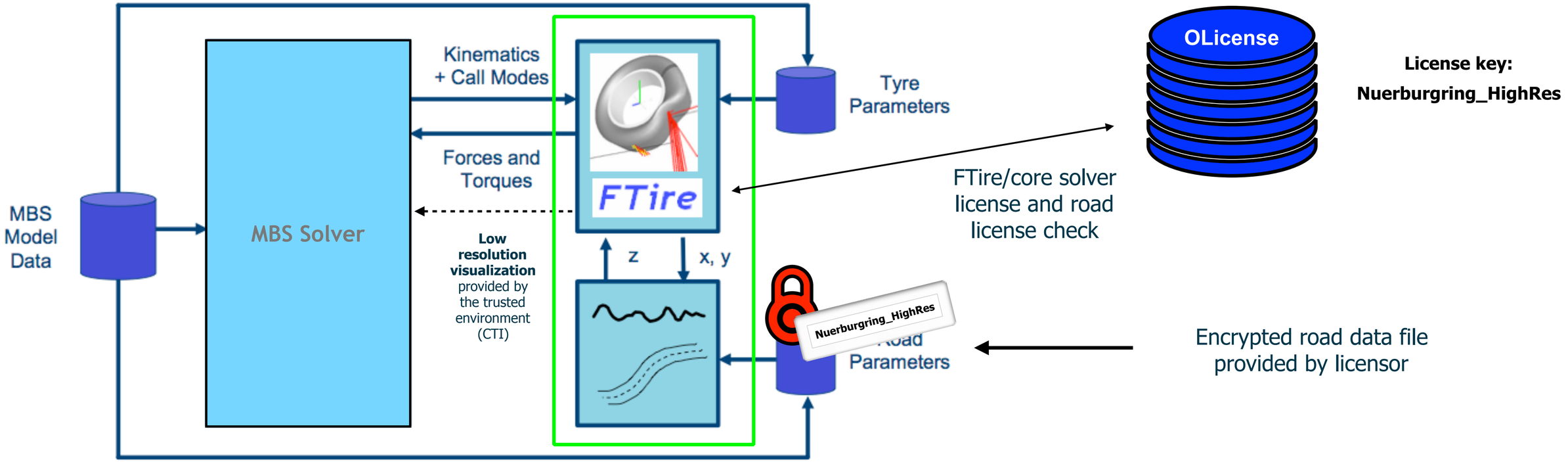
cosin
scientific software

Deployment of DRM protected road data

For the end user, actually there is nothing to observe after the license has been installed. Road data decryption is handled at simulation start automatically, just like the FTire/core solver license check is done.

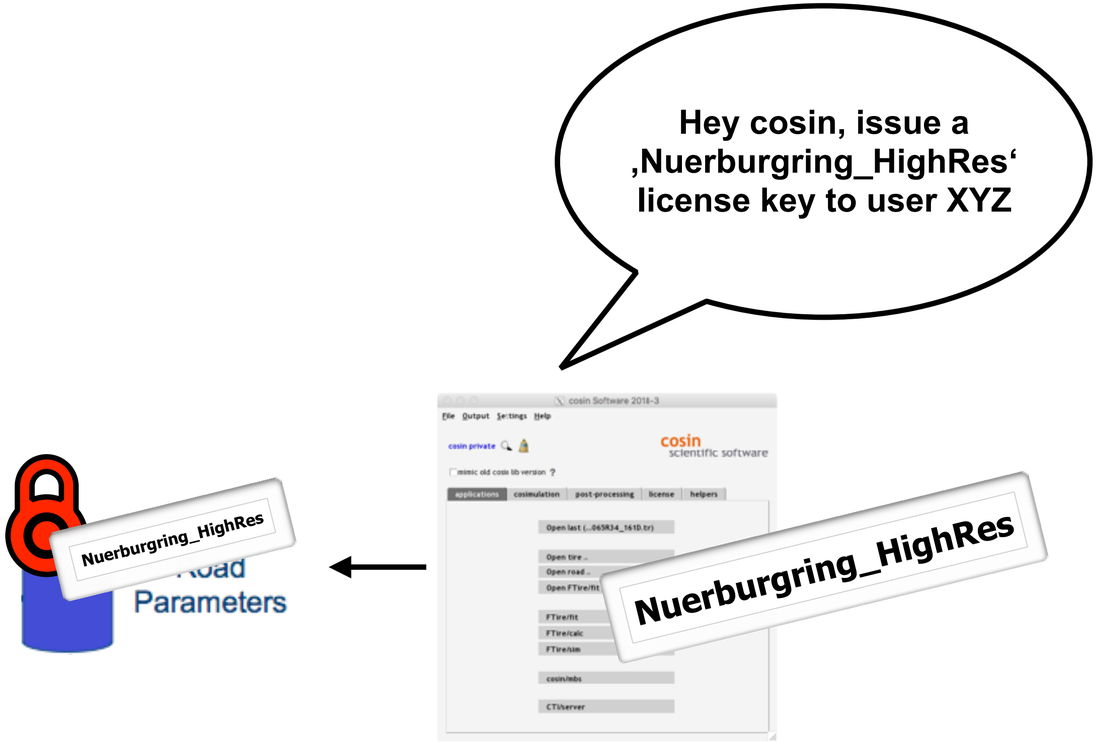
Road data license file provided by cosin on behalf of licensor.

The license file is added to the existing cosin license server.



License ordering process for licensors

- Encryption can be done using cosin/tools.
- Existing data can be encrypted by arbitrary name tags to put single road files under one license key, or even have groups of files sharing the same name tag.
- Road data DRM will be available from cosin release 2018-3.
- Licenses are issued by cosin upon request by the licensor.



cosin/tools

Thank you very much for your attention !