Proposal for SPDX 3.0

"Profile for SCM"
Manage licenses compatible with the final product and clarify responsibility in the supply chain

OpenChain Japan WG
License Info Exchange SWG
Masato ENDO

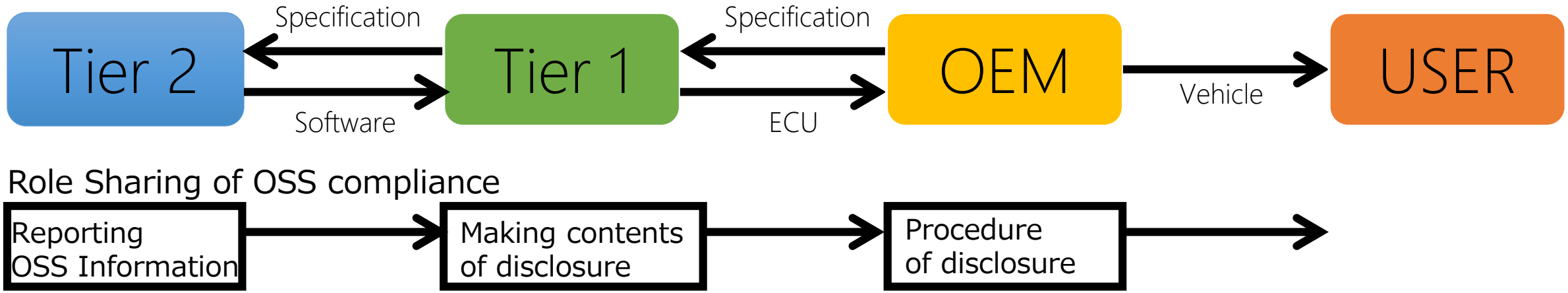
<What is this? >
Profiles to meet the needs of end product manufacturers and suppliers

<Who uses it? >
Profiles used for closed information sharing only in the supply chain

<Advantages for User>
It is attractive that it can be handled in machine-readable SPDX format

<Advantages for SPDX project>
By including information that can be used in actual business use cases, promote using SPDX format

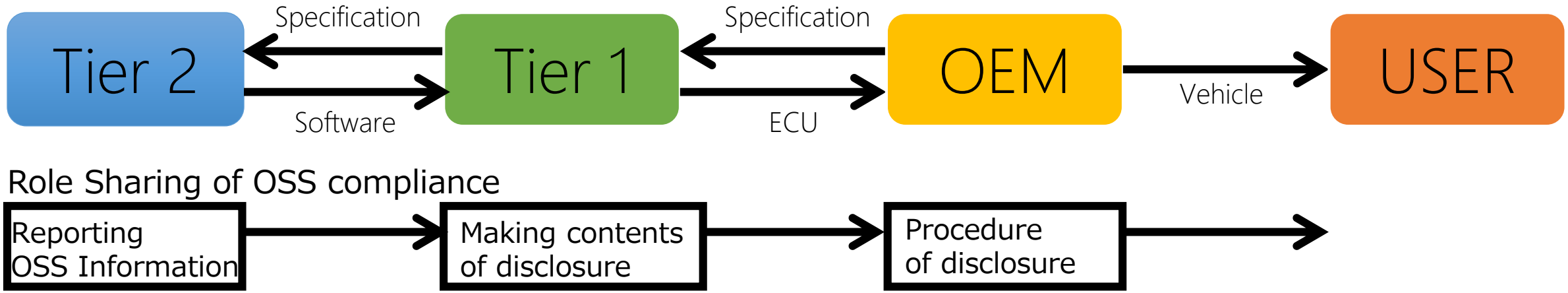
Case of Embedded Software for Automobile



<Constraint condition>

- OEM / Tier1 may not be able to obtain source code for contract reasons
- OEM / Tier1 specifies non-compatible software (package / license) by specification for security reasons
- Tier1 / Tier2 may temporarily use non-compatible software for prototyping purposes

Case of Embedded Software for Automobile



<Tasks for OSS management>

- OEM / Tier1 periodically checks during the development period whether the software includes non-compatible software in the specifications
- If software that is not compatible is included, identify the OSS adopter and implement the replacement
- Manage replacement schedules when temporarily using non-compatible software
- Before the development is completed, Tier 1 collects OSS information of Tier 2 and later, creates contents to be disclosed to USER, and releases to OEM

⇒ Perform the above tasks by routing SBOM (such as SPDX) in the supply chain

⇒If the SBOM contains the necessary information for the above tasks, it can be performed more smoothly

Case of Embedded Software for Automobile

＜information for managing licenses compatible with the final product and clarifying responsibility in the supply chain＞

Information of “Report”
- Reporting day
- Reporter’s name
- Product information (Product name, product number, etc.)
- Schedule of next report

Information of “Compatibility for final product”
- Compatible license with final product or not
- Who adopted the package
- When adopted the package

Information of “Temporary using incompatible software”
- Temporary adoption or using for Final Product (If the package is temporary adoption)
- The schedule of remove
- Who has the responsibility of remove