WIND™

Navigating the Open Source Legal Maze

Best Practices in Linux License and Export Compliance

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

As open source software rapidly becomes central to the development of applications and devices, companies need to be aware of licensing compliance and export disclosure requirements. These issues must be addressed early in the supply chain or there can be costly repercussions for downstream customers—fees and fines, business disruption, even lawsuits. Fortunately, standards are emerging that can streamline the process and ensure all parties are on the same page as software-powered products progress through development. This paper sets forth several important practices for meeting legal requirements, controlling costs, and reducing risks.

TABLE OF CONTENTS

MORE OPEN SOURCE MEANS MORE DISCLOSURE

Open source software (OSS) is everywhere. Linux in particular has moved into the mainstream of software product development. In their "2016 Future of Open Source Survey," Black Duck® Software reported that 65% of respondents are leveraging OSS to speed application development, and 55% use it for production infrastructure. In the Internet of Things (IoT) sector, open source typically accounts for at least 80% of the software in embedded devices, and virtually every IoT device now is being designed and developed with open source technology. In fact, open source permeates the entire end-to-end IoT platform—from sensors to devices, gateways, networks, and the cloud.

There is little doubt, then, that OSS will soon account for the lion's share of software in commercial applications and devices. What that means, however, is that each supply chain participant has to demonstrate compliance with the licensing terms for all OSS used in products delivered to customers. Specifically, they are required to identify each OSS component used, disclose the modifications made, and provide the customer with the source code and licensing data for the software. Just a few years ago, when there was far less open source software being used in development, this was less of an issue for developers. Today, however, there may be hundreds of open source components in a given software product or device. That means accounting for hundreds of license obligations and restrictions.

Accurate tracking of OSS in a product is a matter of quality control. With many players involved in building a software-powered product from initial design to final release, everyone in the supply chain needs complete insight into a product's contents. If there is a problem with the end product, it is crucial to be able to trace the cause to find out where in the chain the problem occurred.

Moreover, if a product is bound for international export there are often requirements regarding the identification and review of the cryptography software used in each open source component—requirements complicated by the fact that different countries have different regulations regarding cryptography. Unless OSS components in the product have been properly accounted for throughout the process, a developer downstream in the supply chain might not be aware of how much cryptography software a product contains.

Companies that downplay compliance and disclosure requirements do so at their peril. The consequences of inadequate documentation of OSS can be severe, including potentially millions in legal damages, fines, and expenses; loss of valuable intellectual property; and loss of revenue if a court halts distribution or authorities deny export rights. Additionally, there are intangible costs like business disruption, lost productivity, and reputational damage.

Wind River® has worked with open source standards organizations to develop uniform approaches to managing OSS license and export compliance. These practices are intended to mitigate the risk of using OSS and avoid the consequences of non-compliance, while relieving developers of the burden of identifying, reporting, and complying with hundreds or even thousands of OSS license terms.

THE COMPLIANCE ENVELOPE BRINGS PEACE OF MIND

To facilitate the sharing of different types of compliance information throughout the supply chain, Wind River introduced the concept of the compliance envelope. A compliance envelope is a zipped archive that contains the following:

- All required licensing data
- Source code legal notices
- Export cryptography information associated with the OSS used to construct the product

The compliance envelope accompanies a product as it is developed, tracing the supply chain from silicon factory to software developer to device manufacturer to device distributor. Each participant in the chain receives all the information needed for understanding a product's composition, adding in more information as it adds functionality to the product. Thus, the compliance envelope's contents are constantly expanding as a product moves from initial development to final distribution.

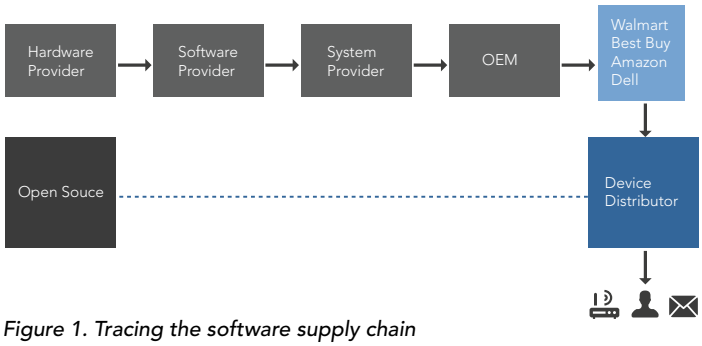


Figure 1. Tracing the software supply chain

LICENSING TERMS

One of the key pieces of information contained in the compliance envelope is the licensing terms of each open source component. The challenge is to ensure the information is consistent in both content and quality from one supplier to the next. Different companies may require different types or levels of licensing data (for example, licensing at the package file level versus the top-level package license). Companies may also have different document format preferences (for example, Microsoft Excel versus PDF). Some may require a list of all copyright holders. Still others may have different definitions of what constitutes open source software, or what an open source license actually covers.

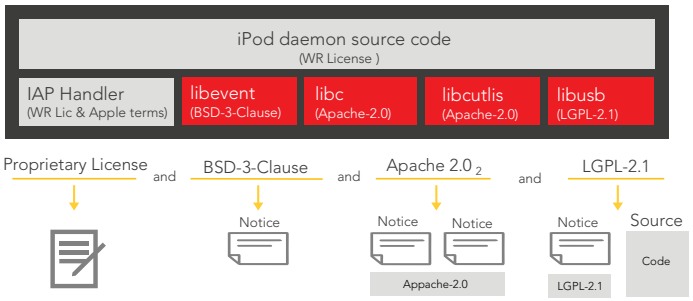


Figure 2. Process example

Since OSS is so widespread in device software development, the industry clearly needs to agree on a standard for the recording and sharing of license information for the many OSS software packages that comprise a product. The Software Package Data Exchange (SPDX) format was designed specifically to address this issue.

SPDX: A STANDARD FOR SHARING LICENSING INFORMATION ACROSS THE SUPPY CHAIN

Developed by the Linux Foundation in collaboration with more than 20 organizations, SPDX is a standard format for communicating the files, components, licenses, and copyrights associated with a software package. The SPDX standard provides a single record of information for each software package, making it easier to comply with OSS license requirements by standardizing the way license information is recorded and shared. With SPDX, licensing data for each source file, library, and program that comprises a software package needs to be identified and recorded only once, eliminating data gaps and duplication of effort on the part of successive members of the chain.

Wind River is among the largest producers of SPDX data. The compliance envelope for Wind River Linux, for example, includes composite license data for the Linux kernel (composed of more than 48,000 files) as well as SPDX files for each of the 1,000-plus OSS packages that make up the total offering. Device manufacturers can then decide which packages are relevant to their needs and gain direct access to the respective licensing data. SPDX is an important first milestone in the movement toward uniform license compliance standards.

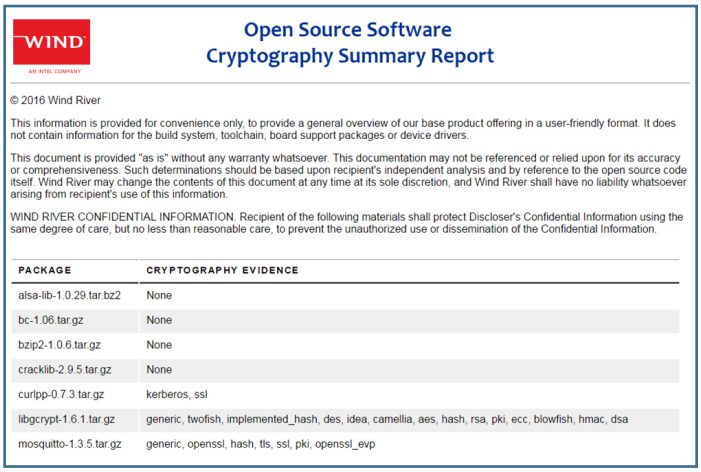
EXPORT COMPLIANCE AND ENCRYPTION DISCLOSURE

Preparing products for international export adds another layer of compliance complexity to the documentation of OSS. In addition to the necessary license compliance requirements, export compliance largely centers around the disclosure of cryptography software, which presents security concerns in many countries. This is an additional reason software suppliers, application developers, and device manufacturers need to have formal processes in place for tracking open source software.

When it comes to documenting OSS in general and cryptography in particular, many technology companies experience a disconnect between the engineering and export teams. Export teams typically expect engineering to know everything in the code base so they can properly report on the cryptography used in a product. If the product has a large number of OSS components and the engineers did not actually write the code, however, they may not have a clear understanding of the cryptography inside.

But export disclosures rely on accurate information from the engineering team, so organizations need to improve the quality of their cryptography discovery in OSS. When there are hundreds or even thousands of OSS components within a product, a manual search is not practical. Some type of automated tool is needed, but automation alone is likely to yield some false positives, which then have to be reviewed manually.

The most efficient solution—the one Wind River employs—is a combination of automation and encryption expertise. First, a tool is used to search the code for encryption, then a designated team trained in encryption technology analyzes the findings to weed out false positives. A report detailing the levels and types of cryptography found is generated and added to the compliance envelope. The export team can then more accurately determine which instances of cryptography need to be reported based on the requirements of the country.



WIND
AN INTEL COMPANY

Open Source Software Cryptography Summary Report

This information is provided for convenience only, to provide a general overview of our base product offering in a user-friendly format. It does not contain information for the build system, toolchain, board support packages or device drivers.

This document is provided "as is" without any warranty whatsoever. This documentation may not be referenced or relied upon for its accuracy or comprehensiveness. Such determinations should be based upon recipient's independent analysis and by reference to the open source code itself. Wind River may change the contents of this document at any time at its sole discretion, and Wind River shall have no liability whatsoever arising from recipient's use of this information.

WIND RIVER CONFIDENTIAL INFORMATION. Recipient of the following materials shall protect Discloser's Confidential Information using the same degree of care, but no less than reasonable care, to prevent the unauthorized use or dissemination of the Confidential Information.

PACKAGE	CRYPTOGRAPHY EVIDENCE
alsa-lib-1.0.29.tar.bz2	None
bc-1.06.tar.gz	None
bzip2-1.0.6.tar.gz	None
cracklib-2.9.5.tar.gz	None
curlpp-0.7.3.tar.gz	kerberos, ssl
libgcrypt-1.6.1.tar.gz	generic, twofish, implemented_hash, des, idea, camellia, aes, hash, rsa, pki, ecc, blowfish, hmac, dsa
mosquitto-1.3.5.tar.gz	generic, openssl, hash, tls, ssl, pki, openssl_evp

Figure 3. Cryptography report outlook

OPENCHAIN BRINGS END-TO-END TRANSPARENCY

With SPDX becoming a standard format for delivering license information, the industry can now move toward a standard definition of compliance quality—those metrics that constitute a stamp of approval on a company's process and output (i.e. the contents of the compliance envelope).

The OpenChain initiative was designed under the leadership of the Linux Foundation to establish exactly this type of quality standard, as well as to foster open source community engagement. It sets forth a number of key requirements to ensure a designated quality level has been achieved. A supplier of software or a developer incorporating OSS must meet all requirements in order to claim OpenChain conformance.

Specific requirements include:

- An open source policy
- A specified level of training on intellectual property topics
- Clearly defined compliance responsibilities within an organization
- A process for identifying, tracking, and archiving all OSS used in a product
- A process of preparing and delivering required compliance artifacts: source code, build scripts, license copies, attribution notices, modification notices, and any other materials required under a specific license agreement

Adherence to OpenChain specification requirements is built into the Wind River product development process. Each project begins with a confirmation that assigned developers have been trained according to the OpenChain specification. All developers are required to disclose the use of OSS, while a team of intellectual property (IP) analysts conducts a review across the development lifecycle. The IP analysts are responsible for determining the obligations under the licenses of the specific OSS used, and for assembling the necessary compliance artifacts to hand off to the release team.

In summary, any Linux vendor—in fact, any participant in the supply chain—should be able to demonstrate a comprehensive, disciplined IP assurance program that includes following the SPDX standard and conforming to the OpenChain specification.

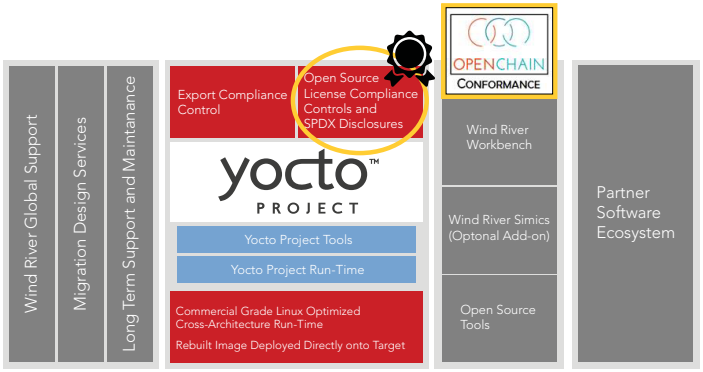


Figure 4. OpenChain conformance in Wind River Linux products

CONCLUSION

License and export compliance have long been afterthoughts to developers using open source software, who are more focused on leveraging Linux to bring products to market quickly. With the proliferation of OSS, however, comes an increased liability risk. And with the rapid expansion of IoT, it is incumbent on developers to assure their customers that applications and devices will perform as promised.

It can be extremely costly and time-consuming for a company's developers to search through all the OSS components in a software product for licensing data. It is far more cost-effective to work with a Linux vendor that adheres to compliance best practices, with a dedicated team focused on meeting OSS licensing and documentation requirements.

A rigorous compliance program, in fact, is part of what distinguishes commercial-grade Linux from OSS simply downloaded from the Internet. Working with a commercial-grade Linux vendor can help ensure an end product that meets not only high quality standards, but demanding legal standards as well.

WIND

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.