5. *Guidelines for software integrity chains and provenance*

The Ericsson Security Reliability Model (SRM) ensures secure software development, delivery, implementation and maintenance across the product lifecycle. Digital cryptographic signing of software, dynamic and static code testing, vulnerability testing, privacy impact analysis and the internal cataloging of libraries and software used, compiled or referenced (e.g. in an SBOM) are fundamental steps to secure software assurance in a mature organization. However, the commercial sensitivity of a Software Bill of Materials (SBOM) dictates that the information that is shared external to the organization is limited to prevent business compromise and security exploitation. It is industry best practice for the software development organization to internally maintain a detailed SBOM such that vulnerability notifications and updates can be properly and safely handled across the installed customer base. Further information about Ericsson's best practice approach to product security and privacy by design are detailed in the following public document:
https://www.ericsson.com/495435/assets/local/security/the-ericsson-security-reliability-model.pdf

Ericsson's position:

- Software should ensure integrity thru digitally signed individual binary packages per product.
- It is the responsibility of every vendor to maintain an internal SBOM to quickly identify a software component with a newly found vulnerability, such as listed in the NVD, determine if that vulnerability is exploitable, assess the impact on the product, and develop and deploy remediations and/or mitigations to such a vulnerability. Advisories should then be issued according to responsible disclosure policies aligned with ISO/IEC 29147:2014.
  Further information about Ericsson's principles of responsible vulnerability disclosure and the Product Security Incident Response Team (PSIRT) responsible for this process are detailed in the following public document:
  https://wcm.ericsson.net/49611c/assets/local/security/psirt-product-security-incident-response-team_rev-a.pdf?_ga=2.197631591.973080165.1621992501-1339862073.1588340656
- Software should provide details of third-party components, including FOSS (Free and Open Source Software). These documents can be shared with regulators/customers/procurement organizations or other stakeholders requesting such details. Internal documented Software Vendor List (SVL) contents are used to extract information on 3rd party components for SBOM purposes.
- Commercial tools are available that can identify FOSS used in binaries and provide a set of detailed information which is similar to that provided in Ericsson customer-available documentation. The accuracy of commercial tools varies considerably, and may result in errors in identifying commercial, proprietary components. Thus, it is Ericsson's recommendation to utilize vendor-provided material which is already accessible to customers through a secure portal authorized for verified customer use.
- An SBOM can contain commercially sensitive content that can be used by competitors to gain business advantages and malicious hackers to exploit known vulnerabilities. SBOMs should be

treated as confidential information. For this reason, Ericsson recommends that the set of required fields is limited to the following and documented in a consistent, repeatable way:

1. Software Component Name
2. Manufacturer
3. Version
4. Country of Origin