Export controls

Contents

Apertis targets a global community, developing products with international reach, and this necessarily makes it interact with the legislation regulating the export of goods, software and technology. In particular, Apertis can be used on products that fall under the "dual-use"categorization since they can be used for both civilian and military applications.

In the context of export controls, it is important to highlight that compliance is a property of a specific product as a whole, and that Apertis being compliant does not automatically translate to products built with Apertis to be compliant. Downstream redistributors and products still need to run their own export control compliance processes.

While Apertis focuses on Open Source software which is largely unrestricted, product teams are likely to deal with proprietary software which may be subject to stronger restrictions, and it is important that the tools and workflow take that in account.

This document aims to provide a high level overview and to identify the tools and workflows that can make such compliance processes easier for product teams.

This document does **not** provide legal advice. It has not been reviewed by any legal team and it only reflects the current best understanding by the development team.

Regulatory framework

This section aims to provide a snapshot (October 2021) of the regulations impacting export of software components, collecting contents from multiple sources in a single place. However, export regulations change relatively quickly so it is recommended to check the actual sources for updates.

Readers can just skim though this section, to get an overall feeling of the regulatory framework that this document tries to address.

European Union

Dual-use trade controls[1] are about goods, software and technology that can be used for both civilian and military applications and refer to (EC) No 2021/821[2] The regulation introduces export controls to ensure compliance of member states to their commitments about "non-proliferation, regional peace, security and stability and respect for human rights and international humanitarian law". In the context of human rights, "cyber-surveillance items"are explicitly listed as subject to controls.

Export control apply also to any transmission directed to cloud services hosted outside the customs territory of the Union. For instance, with the Apertis GitLab being hosted in the EU customs territory, running a job that checks out code from it on a runner hosted in the US would qualify as export.

How export is defined

From article 2 of (EC) No 2021/821[3]:

- a. an export procedure within the meaning of Article 269 of the Union Customs Code[4] ("Union goods to be taken out of the customs territory of the Union");
- b. a re-export within the meaning of Article 270 of the Union Customs Code[5] ("Non-Union goods to be taken out of the customs territory of the Union");
- c. an outward processing procedure within the meaning of Article 259 of the Union Customs Code[6] ("Union goods temporarily exported from the customs territory of the Union in order to undergo processing operations") or
- d. transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the customs territory of the Union; it includes making

[1] https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/
[2] https://eur-lex.europa.eu/eli/reg/2021/821/oj
[3] https://eur-lex.europa.eu/eli/reg/2021/821/oj#002
[4] https://eur-lex.europa.eu/eli/reg/2013/952/oj#269
[5] https://eur-lex.europa.eu/eli/reg/2013/952/oj#270
[6] https://eur-lex.europa.eu/eli/reg/2013/952/oj#259

available in an electronic form such software and technology to natural or legal persons or to partnerships outside the customs territory of the Union; it also include the oral transmission of technology when the technology is described over a voice transmission medium;

Which restrictions apply

Annex 1 of EC) No 2021/821[7] lists the dual-use items for which an authorization is required for export out of the European Union. Items meant to be part of weapons or for cyber-surveillance are also subject to authorization even if not listed in Annex 1. Annex 4 lists dual-use items that are subject to authorization for intra-Union transfers.

Authorizations can be of the following kinds:

- a. Individual licenses that can be granted by competent authorities to one exporter and cover exports of one or more dual-use items to one end-user or consignee in a third country.
- b. Global licenses that can be granted by competent authorities to one exporter and may cover multiple items to multiple countries of destination or end users.
- c. National General Export Authorizations (NGEAs)
- d. EU General Export Authorizations (EUGEAs) allow exports of dual-use items to certain destinations under certain conditions (see Annex II of the Regulation). Regulation (EU) 2021/821 provides for the following EUGEAs:
    1. exports to Australia, Canada, Iceland, Japan, New Zealand, Norway, Switzerland, Liechtenstein, United Kingdom and the United States of America
    2. export of certain dual-use items to certain destinations
    3. export after repair/replacement
    4. temporary export for exhibition or fair
    5. telecommunications
    6. chemicals
    7. intra-group technology transfers
    8. encryption

Detailed registries of exports of dual-use items must record:

- a. a description of the dual-use items;
- b. the quantity of the dual-use items;
- c. the name and address of the exporter and of the consignee;
- d. where known, the end-use and end-user of the dual-use items.

The General Software Note (GSN) in Annex 1 excludes the following software typologies:

[7] https://eur-lex.europa.eu/eli/reg/2021/821/oj#d1e63-25-1

- a. Generally available to the public by being:
    1. Sold from stock at retail selling points, without restriction, by means of: a. Over-the-counter transactions; b. Mail order transactions; c. Electronic transactions; or d. Telephone call transactions; and
    2. Designed for installation by the user without further substantial support by the supplier;
- b. "In the public domain"; or
- c. The minimum necessary "object code"for the installation, operation, maintenance (checking) or repair of those items whose export has been authorized.

Annex 1 of EC) No 2021/821[8] also states in its definitions that "In the public domain"means "technology"or "software"which has been made available without restrictions upon its further dissemination (copyright restrictions do not remove "technology"or "software"from being "in the public domain").

The General "Information Security"Note (GISN) in Annex 1 mandates that "Information security"items or functions should be considered against the provisions in Category 5, Part 2, even if they are components, "software"or functions of other items.

Category 5 covers Telecommunications and Information Security, with part 1 addressing Telecommunications and part 2 addressing Information Security.

The Telecommunications equipment described in Category 5 part 1 specifically focuses on items specially hardened, underwater equipment, high power radio transmission, and other specific use-cases. Civil cellular radio-communications systems are explicitly excluded.

Category 5, part 2 of Annex defines the "Information Security"dual-use items.

The "Cryptography Note"states that 5A002, 5D002.a.1., 5D002.b. and 5D002.c.1. do not control items as follows:

- a. Items that meet all of the following:
    1. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
        - a. Over-the-counter transactions;
        - b. Mail order transactions;
        - c. Electronic transactions; or
        - d. Telephone call transactions;
    2. The cryptographic functionality cannot easily be changed by the user;
    3. Designed for installation by the user without further substantial support by the supplier; and
    4. When necessary, details of the goods are accessible and will be provided, upon request, to the competent authorities of the EU Member State in which the exporter is established in order to ascertain compliance with conditions described in paragraphs 1. to 3. above;

[8] https://eur-lex.europa.eu/eli/reg/2021/821/oj#d1e63-25-1

- b. Hardware components or 'executable software', of existing items described in paragraph a. of this Note, that have been designed for these existing items, meeting all of the following:
    1. "Information security"is not the primary function or set of functions of the component or 'executable software';
    2. The component or 'executable software'does not change any cryptographic functionality of the existing items, or add new cryptographic functionality to the existing items;
    3. The feature set of the component or 'executable software'is fixed and is not designed or modified to customer specification; and
    4. When necessary as determined by the competent authorities of the EU Member State in which the exporter is established, details of the component or 'executable software'and details of relevant end-items are accessible and will be provided to the competent authority upon request, in order to ascertain compliance with conditions described above.

For the purpose of the Cryptography Note, 'executable software'means "software" in executable form, from an existing hardware component excluded from 5A002 by the Cryptography Note. 'Executable software'does not include complete binary images of the "software"running on an end-item.

Note 2 excludes:

- a. Smart cards and smart card 'readers/writers'
- b. Cryptographic equipment specially designed and limited for banking use or 'money transactions';
- c. Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radio communication systems) that are not capable of transmitting encrypted data directly to another radiotelephone or equipment (other than Radio Access Network (RAN) equipment)
- d. Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation
- e. Portable or mobile radiotelephones and similar client wireless devices for civil use, that implement only published or commercial cryptographic standards (except for anti-piracy functions, which may be non-published) and also meet the provisions of paragraphs a.2. to a.4. of the Cryptography Note
- f. Items, where the "information security"functionality is limited to wireless "personal area network"functionality, implementing only published or commercial cryptographic standards;
- g. Mobile telecommunications Radio Access Network (RAN) equipment designed for civil use, which also meet the provisions of paragraphs a.2. to a.4. of the Cryptography Note
- h. Routers, switches, gateways or relays, where the "information security"functionality is limited to the tasks of "Operations, Administration or Maintenance"("OAM") implementing only published or commercial cryp-

tographic standards; or

- i. General purpose computing equipment or servers, where the "information security"functionality meets all of the following:
  1. Uses only published or commercial cryptographic standards; and
  2. Is any of the following:
     - a. Integral to a CPU that meets the provisions of Note 3 to Category 5, Part 2;
     - b. Integral to an operating system that is not specified in 5D002; or
     - c. Limited to "OAM"of the equipment.
- j. Items specially designed for a 'connected civil industry application', meeting all of the following:
  1. Being any of the following:
     - a. A network-capable endpoint device meeting any of the following:
       (a) The "information security"functionality is limited to securing 'non-arbitrary data'or the tasks of "Operations, Administration or Maintenance"("OAM"); or
       (b) The device is limited to a specific 'connected civil industry application'; or
     - b. Networking equipment meeting all of the following:
       (a) Being specially designed to communicate with the devices specified in paragraph j.1.a. above; and
       (b) The "information security"functionality is limited to supporting the 'connected civil industry application'of devices specified in paragraph j.1.a. above, or the tasks of "OAM"of this networking equipment or of other items specified in paragraph j. of this Note; and 2. Where the "information security"functionality implements only published or commercial cryptographic standards, and the cryptographic functionality cannot easily be changed by the user.

In general, section D for each of the categories in Annex 1 is meant to catalog the software that implements or is used to develop or control the dual-use items described in each category: for instance, 5D001 and 5D002 are the codes for software related to Category 5 "Telecommunications and Information Security" , part 1 "Telecommunications"and part 2 "Information Security"respectively.

United States

The Bureau of Industry and Security (BIS)[9] is the entity that enforces the Export Administration Regulations (EAR)[10], governing the export and re-export of goods, software, and technology, including dual-use items that can be used both for commercial and military purposes.

[9] https://www.bis.doc.gov/

[10] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734

How export is defined

The EAR defines "export"[11] as:

- a. With specific exceptions, Export means:
    1. An actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner;
    2. Releasing or otherwise transferring "technology"or source code (but not object code) to a foreign person in the United States (a "deemed export");
    3. Transferring by a person in the United States of registration, control, or ownership of a spacecraft under certain circumstances;
- b. Any release in the United States of "technology"or source code to a foreign person is a deemed export to the foreign person's most recent country of citizenship or permanent residency.
- c. The export of an item that will transit through a country or countries to a destination identified in the EAR is deemed to be an export to that destination.

Similarly, "re-export"is defined[12] as:

- a. With specific exceptions, Reexport means:
    1. An actual shipment or transmission of an item subject to the EAR from one foreign country to another foreign country, including the sending or taking of an item to or from such countries in any manner;
    2. Releasing or otherwise transferring "technology"or source code subject to the EAR to a foreign person of a country other than the foreign country where the release or transfer takes place (a deemed reexport);
    3. Transferring by a person outside the United States of registration, control, or ownership of a spacecraft under certain circumstances;
- b. Any release outside of the United States of "technology"or source code subject to the EAR to a foreign person of another country is a deemed reexport to the foreign person's most recent country of citizenship or permanent residency, except under certain circumstances.
- c. The reexport of an item subject to the EAR that will transit through a country or countries to a destination identified in the EAR is deemed to be a reexport to that destination.

Exceptions explicitly cover encryption source code and object code software[13] and other general activities that are not subject to the regulation[14].

[11] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734#734.13

[12] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734#734.14

[13] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734#734.17

[14] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-

Which restrictions apply

Ten General Prohibitions[15] defines the activities for which a license from BIS is required. The Commerce Control List[16] defines the categories of items subject to the authority of BIS.

Category 5 of the Commerce Control List covers Telecommunications and Information Security

Relevant details about encryption source code and object code software[17] are:

- b. The export of encryption source code and object code "software"controlled for "EI"reasons under ECCN 5D002 on the Commerce Control List includes:
    1. Downloading, or causing the downloading of, such "software"to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or
    2. Making such "software"available for transfer outside the United States, over digital communication channels, unless the person making the "software"available takes precautions adequate to prevent unauthorized transfer of such code. Publicly available encryption source code "software"and corresponding object code are not subject to the EAR only when the encryption source code "software"meets specific additional requirements.
- c. precautions for Internet transfers of products eligible for export under § 740.17(b)(2) of the EAR (encryption "software"products, certain encryption source code and general purpose encryption toolkits) shall include such measures as:
    1. The access control system, either through automated means or human intervention, checks the address of every system outside of the U.S. or Canada requesting or receiving a transfer and verifies such systems do not have a domain name or Internet address of a foreign government end-user (e.g., ".gov,"".gouv,"".mil"or similar addresses);
    2. The access control system provides every requesting or receiving party with notice that the transfer includes or would include cryptographic "software"subject to export controls under the Export Administration Regulations, and anyone receiving such a transfer cannot export the "software"without a license or other authorization; and
    3. Every party requesting or receiving a transfer of such "software"must acknowledge affirmatively that the "software"is not intended for use by a government end user and he or she understands the cryptographic "software"is subject to export controls under the Export Administration Regulations and anyone receiving the transfer cannot

734#734.18

[15] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-736

[16] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-774

[17] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734#734.17

export the “software”without a license or other authorization. BIS will consider acknowledgments in electronic form provided they are adequate to assure legal undertakings similar to written acknowledgments.

The Encryption commodities, software, and technology (ENC)[18] license exception authorizes export of software and technology classified under 5D002 or 5E002. It states that “No classification request or reporting required”applies to “Certain exports, reexports, transfers (in-country) to ‘private sector end users’” , including “internal “development”or “production”of new products”[19]. In other cases immediate authorization is granted[20] for items classified under 5D002 after the submissions of a self-classification report[21] to crypt-supp8@bis.doc.gov[22] and to enc@nsa.gov[23] in a CSV spreadsheet[24] with a specific set of information[25].

Export control and OSS

The EU General Software Note (GSN) in Annex 1 of (EC) No 2021/821[26] excludes software “in the public domain”from what should be subject to export authorizations and the updated EU dual use control list (EU) 2020/1749[27] clarifies that “in the public domain”refers to software that is available without restrictions upon its further dissemination and that copyright restrictions in this context do not remove software from the public domain. This seem to indicate that for the EU regulations all the Open Source Software is exempt from export controls, regardless of its purpose.

As pointed out by the official US BIS guidance[28], the changes to the rules on 2021-Mar-29[29] have eliminated the e-mail notification requirement for ‘publicly available’encryption source code and beta test encryption software, except for

[18] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-740#740.17

[19] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-740#p-740.17%28a%29%281%29%28i%29

[20] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-740#p-740.17%28b%29%281%29

[21] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-740#p-740.17%28e%29%283%29

[22] mailto:crypt-supp8@bis.doc.gov

[23] mailto:enc@nsa.gov

[24] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-740#p-740.17%28e%29%283%29%28iv%29

[25] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-742#Supplement-No.-8-to-Part-742

[26] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:206:FULL&from=EN

[27] https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159198.pdf

[28] https://www.bis.doc.gov/index.php/policy-guidance/encryption

[29] https://www.bis.doc.gov/index.php/component/docman/?task=doc_download&gid=2759

software implementing "non-standard cryptography"[30], defined as any implementation of "cryptography"involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, and GSMA) and have not otherwise been published.

Accordingly to the Linux Foundation, this removes the notification requirements for most products based on OSS projects[31].

On that ground, the assumption in this document is that any product based on Apertis is exempt from the notification requirement except for very uncommon scenarios where custom cryptography is used by the product itself. This also applies to downstreams rebuilding the Apertis sources, as long as they do not introduce custom cryptographic algorithms and proprietary implementations.

Sample export control compliance vendor process

The goal with export compliance in Apertis is to focus on the following use-cases:

- **UC1**: Processing of ECCN classified packages/components in downstream Apertis distributions for which an export notification has to be given to legal authorities (e.g. 5D classified)
- **UC2**: Processing of ECCN classified packages/components in downstream Apertis products for which an export notification has to be given to legal authorities (e.g. 5D classified)
- **UC3**: Processing of ECCN classified packages/components in downstream Apertis distributions for which an approval from legal authorities is required before getting exported (5E classified)
- **UC4**: Processing of ECCN classified packages/components in downstream Apertis products for which an approval from legal authorities is required before getting exported (5E classified)
- **UC5**: Handle changed ECCN classification of already added components (5D to 5E, 5E to 5D, classified to unclassified, unclassified to classified) in downstream Apertis distributions and products
- **UC6**: Handle SW components where the ECCN classification is different for the binary and the source code

The basic requirements are:

1. Apertis and projects based on it have to handle SW components covered under export control regulations
2. Some ECCN classified (5D) SW components require a listing of legal entities and countries to which these SW components got exported, the listing

[30] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-772

[31] https://www.linuxfoundation.org/resources/publications/understanding-us-export-controls-with-open-source-projects/

has to be provided to the export control authorities
3. Some ECCN classified (5E) SW components are not allowed to be exported without prior approval from the export control authorities
4. Within the vendor worldwide, the announcements, notifications and approval requests exchanged with the legal authorities in the countries are often centrally organized worldwide by a specific department
5. Beside delivering SW products the export of SW also encompasses sharing and providing SW via links to repositories for any other party and persons to access, download and further usage.

ECCN numbers for SW components can be assumed as given, no detection mechanism is needed.

Assessment questionnaire

The form below provides an example of the information that product teams need to collect about their software components to decide whether a closer inspection is needed or not, in case they need to be classified for export.

- **Producer**
  Emmett Brown SpA
- **Name and version**
  Embedded Software for Flux Capacitor 42A
- **Licensor (Vendor-contract partner)**
  End User
- **Main function of the software**
  Operation of flux dispersal device Flux Capacitor 42A. The software is used for data acquisition, signal processing and flux capacitance management. Cryptography is used to protect the company IP, by encrypting and signing the update files which can be installed by the user. Encryption/Singing is also used to restrict the access to the operating system command line, used for development and production.

1. Central clearing over Software Consulting Service (SCS) (planned)?
   Yes: Indication of PID
   No

2. Indications concerning type of software
   Licensed software
   Freeware
   Open Source Software (OSS)
   Central Directive “Handling Open Source Software”is complied with:
   Yes No

3. Are there indications concerning export control restrictions by the producer/distributor/provider or in the license agreement?
   Yes
   Indication of Export Control List Number, ECCN, EAR99:

- *https://wiki.debian.org/USExportControl Some parts of Debian such as cryptographic softwares may be covered under ECCN 5D002. However, those parts are likely to fall under the TSU license exception. If this is true, no license is required to export products using such parts.*

No

4. Supply by electronic media?
   Yes
   Indication of provision source and if so Internet link:
   - *http://example.com/products/flux/src/*

   No
5. Employment of cryptographic algorithms?
   Yes
   Indication of type of cryptography (symmetric/asymmetric) and key length:
   No
6. Which of the following functions/characteristics apply for the software?
   Encryption for the protection of intellectual property and personal data and not user-accessible (encryption / signing of update files)
   Authentication function only (SSH login)
   Mass-Market-Criteria
   SSL / https
   none
7. Has the software been appliqued or changed for military use?
   Yes
   No
8. Open Source Software [Only to be filled out in case of OSS as stand-alone or integrated in products]
   - Which kind of license applies for the OSS? Indication of license type (e.g. GPL, CPL, MPL, LGPL):
     - *Open SSH v7.9: BSD-Berkeley Software License Agreement, ISC, BSD-2-Clause*
     - *Open SSL v1.1.1: SSL-license, SSLeay License*
     - *libcryptsetup12 v2.1.0: GLPv2 / LGPLv2*
     - *libblockdev-crypto2 v2.20: LGPL-2.1+*
     - *gnupg v1.4.7: GPL2.0+*
     - *libcrypt20 v1.8.4: LGPLv2.1+*
     - *krb5 v1.17: MIT*
     - *nettle v3.2: LGPL-3.0+ or GPL-2.0+*
     - *NSS v3.42: MPL 2.0*
     - *P11-kit v0.23: BSD-3-Clause*

  - *Cyrus-sasl2 v2.1.27: BSD 3 clause*
  - *Libsecret v0.18.7: LGPLv2.1+*
  - *Libsodium v1.017: ISC / BSD 2-clause / CC0 / MIT*
  - *Volume-key v0.3.12: GPLv2*
  - *Linux Kernel v4.19: GPLv2*
  - *Shadow v4.5: BSD 2 / 3 clause / GPLv2.0+*
- Is the company required to provide the OSS as license term?
  Yes
  No

9. Which criteria apply concerning US-reexport legislation?

- Has the software been imported from the US/manufactured in the US or is the producer/licensor a US-company?
  Yes
  No
- Has the software been produced based on listed US-software / US-technology?
  Yes
  Indication of programming environment and export control list number:
  EAR99 ECCN 5D992 ECCN 5D002
  No

- Result of assessment:
- List number:
  - National:
  - US Re-export control: EAR99 ECCN 5D992 ECCN 5D002 Direct product
  - Date:
  - ECO:

Purchased SW ECCN classification list

Once all components used on a specific product have been acquired and classified, it is necessary to list their details to get approval for export of the product as a whole.

- SW component

Name of the SW component	Target Processor	Details [optional]
Flux Capacitor Classic	RH850	Gen3 Platform

- SW-Vendor address

Name	Street	No	Post Code	City	Country
Emmett Brown Flux Components	Piazza San Carlo	42	10121	Torino	Italy

- SW-Vendor contacts

Contact Person we got/will get ECCN information from	Mail	Phone	Nam
Jane Doe	Jane.Doe@example.com	+39 555 1234567	n.a.

- SW delivery from SW-vendor to Vendor

Source Code or Binary	Delivery date	Country the SW was delivered to? (in some cases it is different to t
source	30/01/2021	Italy

- Export Information

  For some 5D classified software it has to be known and reportable from which countries and legal entities the SW component can be accessed, considering both source and binary files.

  5E classified source and binary files in general are subject to authorization **before** doing any export. After approval from the authorities, these 5E files can be exported/enabled for access for the approved country and legal entity. Especially if a 5E component is approved for export/access to a country/legal entity, e.g. for development, and afterwards another country or legal entity also needs to work with this 5E component, it also has to be approved before using for development and other work. In some situations, there may be an intermediate solution required to not block the complete development.

ECCN for the SW component	Date of ECCN classification	Countries with access to the server location w
5D992.c	30/05/2021	India, Malaysia, China, Vietnam

- Vendor internal Software Subcontractormanager

Name	Department	Phone	Legal Vendor entity (e.g. EBEI, EBVH)	Site
Jim Smith	EBEI/FC	+39 555 7654321	EBCM	To

- Other

Comment	Who filled this entry to this table? (if not Subcontractor manager)	Date when it was fille
Example entry	Paolo Rossi	30/09/2021

Approach

Classifications always happens in the context of a specific product, so it is not possible to provide generally-valid metadata in re-usable software repositories.

However, each software package can provide hints to guide the classification process to make it easier and reduce the chance of errors.

Each package can thus provide export control metadata such as ECCNs and intended access controls: the metadata is associated to source and binary packages, no finer-grained granularity is in scope. Multiple ECCNs can be provided since in some cases they need to change depending on how the final product is distributed: for instance, software under 5D002 may need to be reclassified as 5D992 when distributed under the mass-market provisions.

It is the responsibility of the maintainer of each software components to assess which export control restrictions apply to their packages and manually capture the output in the packages metadata.

The metadata is used when deployable software images and updates are built, to automatically generate a raw software bill of materials (SBOM) listing the packages that are shipped in each software artifact, their licenses, their location, and their associated export control information.

The SBOM is then used as the input for the product level assessment to be submitted to the department responsible for export control handling.

Package metadata

The metadata is going to be maintained alongside the other packaging metadata and sources, to be shipped with each binary package and made available at image build time.

The exact format of the metadata is to be defined, but it is going to be based on a text-based, machine-readable syntax (JSON, deb822, YAML). The metadata can be made available in dedicated files under `/usr/share/doc` similarly to what the licensing workflow currently does, or even directly in the .deb `debian/control` metadata.

The metadata shipped with each binary package will provide the following information:

- potentially appliable ECCNs
- for each ECCN, a short rationale for the categorization

- for 5D002 and 5D992, whether non-standard cryptography is also implemented
- for restricted components, countries with access
- for restricted components, legal entities with access

Software bill of materials

For each produced artifacts (base OS images, update bundles, container images, app bundles) a SBOM is produced, listing the information below about each binary package installed:

- binary package name
- binary package version
- source package name
- source package version
- binary package ECCNs
  - for each ECCNs a rationale is provided
  - for 5D002 and 5D992, whether non-standard cryptography is also used
- link to binary package
- link to source
- countries with access
- legal entities with access

Artifacts recipes can provide additional metadata to group packages by the purpose they are actually used for on the artifacts. For instance, this is valuable to provide more insight about the actual use of cryptography for packages providing generic cryptographic services like OpenSSL or the Linux kernel, where the package metadata is going to be necessarily too generic for an appropriate evaluation in the context of the specific product.

An hypotetical example of such metadata could be:

```
- purpose: Command line access during development
  packages: [ openssh-server ]
  non-standard-cryptography: false
- purpose: HTTPS connectivity for OTA updates and telemetry
  packages: [ libssl1.1, libnettle8, libgnutls ]
  non-standard-cryptography: false
- purpose: Software updates integrity and confidentiality
  packages: [ libssl1.1 ]
  non-standard-cryptography: false
- purpose: Device integrity
  packages: [ "linux-image-*", libcryptsetup12 ]
  non-standard-cryptography: false
```

By grouping packages in the SBOM by the provided purposes more product-specific context is provided to evaluate the use of categorized components.

Access control and audit

Access controls are managed at the user level using the access control mechanism already provided by each service (GitLab, OBS, etc.), for the moment no further access control or auditing log is planned.

This means that it is responsibility of each user to ensure the code is retrieved only when connecting from authorized countries.

Further restrictions enforcing per-request GeoIP checks and more detailed audit logs may be investigated and implemented in the future.

An important provision is about ensuring that the cloud services used to host the Apertis services are all hosted in the same customs territory to avoid transmissions that may be subject to export controls. This can be controlled by choosing carefully the geographic zone when instantiating cloud services. It may be worth considering making the zone part of the naming scheme for GitLab runners, OBS worker and LAVA dispatchers, and also ensure they are tagged appropriately to ensure product teams can control where their code gets checked out.

Generally speaking, it is recommended to ensure restricted components do not make any use of shared runners/workers/dispatchers and all their workload are handled by dedicated instances with the appropriate tags.

All the Apertis services are currently based in the EU and UK customs territory, with the LAVA testing infrastructure in particular being hosted in the UK. An analysis of the impact of Brexit will be required to understand which actions need to be taken to avoid export-related issues.