



Export controls

Contents

2	Regulatory framework	3
3	European Union	3
4	How export is defined	3
5	Which restrictions apply	4
6	United States	7
7	How export is defined	8
8	Which restrictions apply	9
9	Export control and OSS	10
10	Sample export control compliance vendor process	11
11	Assessment questionnaire	12
12	Purchased SW ECCN classification list	14
13	Approach	16
14	Package metadata	16
15	Software bill of materials	17
16	Access control and audit	18

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.

36 Regulatory framework

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

41 Readers can just skim through this section, to get an overall feeling of the regu-
42 latory framework that this document tries to address.

43 European Union

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

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

55 How export is defined

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

- 57 • a. an export procedure within the meaning of [Article 269 of the Union](#)
58 [Customs Code](#)⁴ (“Union goods to be taken out of the customs territory of
59 the Union”);
- 60 • b. a re-export within the meaning of [Article 270 of the Union Customs](#)
61 [Code](#)⁵ (“Non-Union goods to be taken out of the customs territory of the
62 Union”);
- 63 • c. an outward processing procedure within the meaning of [Article 259 of](#)
64 [the Union Customs Code](#)⁶ (“Union goods temporarily exported from the
65 customs territory of the Union in order to undergo processing operations”
66) or
- 67 • d. transmission of software or technology by electronic media, including
68 by fax, telephone, electronic mail or any other electronic means to a des-
69 tination 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 2021/821⁷](#) 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>

- 109 • a. Generally available to the public by being:
 - 110 1. Sold from stock at retail selling points, without restriction, by means
 - 111 of: a. Over-the-counter transactions; b. Mail order transactions; c.
 - 112 Electronic transactions; or d. Telephone call transactions; and
 - 113 2. Designed for installation by the user without further substantial sup-
 - 114 port by the supplier;
- 115 • b. “In the public domain”; or
- 116 • c. The minimum necessary “object code” for the installation, operation,
- 117 maintenance (checking) or repair of those items whose export has been
- 118 authorized.

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

123 The General “Information Security” Note (GISN) in Annex 1 mandates that “In-
 124 formation security” items or functions should be considered against the provi-
 125 sions in Category 5, Part 2, even if they are components, “software” or functions
 126 of other items.

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

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

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

134 The “Cryptography Note” states that 5A002, 5D002.a.1., 5D002.b. and
 135 5D002.c.1. do not control items as follows:

- 136 • a. Items that meet all of the following:
 - 137 1. Generally available to the public by being sold, without restriction,
 - 138 from stock at retail selling points by means of any of the following:
 - 139 – a. Over-the-counter transactions;
 - 140 – b. Mail order transactions;
 - 141 – c. Electronic transactions; or
 - 142 – d. Telephone call transactions;
 - 143 2. The cryptographic functionality cannot easily be changed by the user;
 - 144 3. Designed for installation by the user without further substantial sup-
 - 145 port by the supplier; and
 - 146 4. When necessary, details of the goods are accessible and will be pro-
 - 147 vided, upon request, to the competent authorities of the EU Member
 - 148 State in which the exporter is established in order to ascertain com-
 - 149 pliance with conditions described in paragraphs 1. to 3. above;

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

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

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

170 Note 2 excludes:

- 171 • a. Smart cards and smart card 'readers/writers'
- 172 • b. Cryptographic equipment specially designed and limited for banking
173 use or 'money transactions';
- 174 • c. Portable or mobile radiotelephones for civil use (e.g., for use with
175 commercial civil cellular radio communication systems) that are not capa-
176 ble of transmitting encrypted data directly to another radiotelephone or
177 equipment (other than Radio Access Network (RAN) equipment)
- 178 • d. Cordless telephone equipment not capable of end-to-end encryption
179 where the maximum effective range of unboosted cordless operation
- 180 • e. Portable or mobile radiotelephones and similar client wireless devices
181 for civil use, that implement only published or commercial cryptographic
182 standards (except for anti-piracy functions, which may be non-published)
183 and also meet the provisions of paragraphs a.2. to a.4. of the Cryptogra-
184 phy Note
- 185 • f. Items, where the "information security" functionality is limited to wire-
186 less "personal area network" functionality, implementing only published or
187 commercial cryptographic standards;
- 188 • g. Mobile telecommunications Radio Access Network (RAN) equipment
189 designed for civil use, which also meet the provisions of paragraphs a.2.
190 to a.4. of the Cryptography Note
- 191 • h. Routers, switches, gateways or relays, where the "information secu-
192 rity" functionality is limited to the tasks of "Operations, Administration or
193 Maintenance" ("OAM") implementing only published or commercial cryp-

194 cryptographic standards; or

- 195 • i. General purpose computing equipment or servers, where the “informa-
196 tion security” functionality meets all of the following:
 - 197 1. Uses only published or commercial cryptographic standards; and
 - 198 2. Is any of the following:
 - 199 – a. Integral to a CPU that meets the provisions of Note 3 to
 - 200 Category 5, Part 2;
 - 201 – b. Integral to an operating system that is not specified in 5D002;
 - 202 or
 - 203 – c. Limited to “OAM” of the equipment.
- 204 • j. Items specially designed for a ‘connected civil industry application’,
205 meeting all of the following:
 - 206 1. Being any of the following:
 - 207 – a. A network-capable endpoint device meeting any of the follow-
208 ing:
 - 209 (a) The “information security” functionality is limited to securing
210 ‘non-arbitrary data’ or the tasks of “Operations, Administra-
211 tion or Maintenance”(“OAM”); or
 - 212 (b) The device is limited to a specific ‘connected civil industry
213 application’; or
 - 214 – b. Networking equipment meeting all of the following:
 - 215 (a) Being specially designed to communicate with the devices
216 specified in paragraph j.1.a. above; and
 - 217 (b) The “information security” functionality is limited to support-
218 ing the ‘connected civil industry application’ of devices speci-
219 fied in paragraph j.1.a. above, or the tasks of “OAM” of this
220 networking equipment or of other items specified in para-
221 graph j. of this Note; and 2. Where the “information secu-
222 rity” functionality implements only published or commercial
223 cryptographic standards, and the cryptographic functional-
224 ity cannot easily be changed by the user.

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

230 United States

231 The Bureau of Industry and Security (BIS)⁹ is the entity that enforces the Ex-
232 port Administration Regulations (EAR)¹⁰, governing the export and re-export
233 of goods, software, and technology, including dual-use items that can be used
234 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>

235 **How export is defined**

236 The EAR defines “export”¹¹ as:

- 237 • a. With specific exceptions, Export means:
- 238 1. An actual shipment or transmission out of the United States, includ-
- 239 ing the sending or taking of an item out of the United States, in any
- 240 manner;
- 241 2. Releasing or otherwise transferring “technology”or source code (but
- 242 not object code) to a foreign person in the United States (a “deemed
- 243 export”);
- 244 3. Transferring by a person in the United States of registration, control,
- 245 or ownership of a spacecraft under certain circumstances;
- 246 • b. Any release in the United States of “technology”or source code to a
- 247 foreign person is a deemed export to the foreign person’s most recent
- 248 country of citizenship or permanent residency.
- 249 • c. The export of an item that will transit through a country or countries
- 250 to a destination identified in the EAR is deemed to be an export to that
- 251 destination.

252 Similarly, “re-export”is defined¹² as:

- 253 • a. With specific exceptions, Reexport means:
- 254 1. An actual shipment or transmission of an item subject to the EAR
- 255 from one foreign country to another foreign country, including the
- 256 sending or taking of an item to or from such countries in any manner;
- 257 2. Releasing or otherwise transferring “technology”or source code sub-
- 258 ject to the EAR to a foreign person of a country other than the
- 259 foreign country where the release or transfer takes place (a deemed
- 260 reexport);
- 261 3. Transferring by a person outside the United States of registration,
- 262 control, or ownership of a spacecraft under certain circumstances;
- 263 • b. Any release outside of the United States of “technology”or source code
- 264 subject to the EAR to a foreign person of another country is a deemed
- 265 reexport to the foreign person’s most recent country of citizenship or per-
- 266 manent residency, except under certain circumstances.
- 267 • c. The reexport of an item subject to the EAR that will transit through
- 268 a country or countries to a destination identified in the EAR is deemed to
- 269 be a reexport to that destination.

270 Exceptions explicitly cover encryption source code and object code software¹³

271 and other general activities that are not subject to the regulation¹⁴.

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-734#734.17>

272 **Which restrictions apply**

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

276 Category 5 of the Commerce Control List covers Telecommunications and In-
277 formation Security

278 Relevant details about **encryption source code and object code software**¹⁷ are:

- 279 • b. The export of encryption source code and object code “software” con-
280 trolled for “EI” reasons under ECCN 5D002 on the Commerce Control List
281 includes:
 - 282 1. Downloading, or causing the downloading of, such “software” to lo-
283 cations (including electronic bulletin boards, Internet file transfer
284 protocol, and World Wide Web sites) outside the U.S., or
 - 285 2. Making such “software” available for transfer outside the United
286 States, over digital communication channels, unless the person mak-
287 ing the “software” available takes precautions adequate to prevent
288 unauthorized transfer of such code. Publicly available encryption
289 source code “software” and corresponding object code are not subject
290 to the EAR only when the encryption source code “software” meets
291 specific additional requirements.
- 292 • c. precautions for Internet transfers of products eligible for export under §
293 740.17(b)(2) of the EAR (encryption “software” products, certain encryp-
294 tion source code and general purpose encryption toolkits) shall include
295 such measures as:
 - 296 1. The access control system, either through automated means or hu-
297 man intervention, checks the address of every system outside of the
298 U.S. or Canada requesting or receiving a transfer and verifies such
299 systems do not have a domain name or Internet address of a foreign
300 government end-user (e.g., “.gov,” “.gouv,” “.mil” or similar addresses);
 - 301 2. The access control system provides every requesting or receiving party
302 with notice that the transfer includes or would include cryptographic
303 “software” subject to export controls under the Export Administration
304 Regulations, and anyone receiving such a transfer cannot export the
305 “software” without a license or other authorization; and
 - 306 3. Every party requesting or receiving a transfer of such “software” must
307 acknowledge affirmatively that the “software” is not intended for use
308 by a government end user and he or she understands the crypto-
309 graphic “software” is subject to export controls under the Export Ad-
310 ministration 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>

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

315 The Encryption commodities, software, and technology (ENC)¹⁸ license excep-
316 tion authorizes export of software and technology classified under 5D002 or
317 5E002. It states that “No classification request or reporting required” applies to
318 “Certain exports, reexports, transfers (in-country) to ‘private sector end users’”
319 , including “internal “development” or “production” of new products”¹⁹. In other
320 cases immediate authorization is granted²⁰ for items classified under 5D002 after
321 the submissions of a self-classification report²¹ to crypt-supp8@bis.doc.gov²²
322 and to enc@nsa.gov²³ in a CSV spreadsheet²⁴ with a specific set of informa-
323 tion²⁵.

324 Export control and OSS

325 The EU General Software Note (GSN) in Annex 1 of (EC) No 2021/821²⁶ ex-
326 cludes software “in the public domain” from what should be subject to export
327 authorizations and the updated EU dual use control list (EU) 2020/1749²⁷ clar-
328 ifies that “in the public domain” refers to software that is available without re-
329 strictions upon its further dissemination and that copyright restrictions in this
330 context do not remove software from the public domain. This seem to indicate
331 that for the EU regulations all the Open Source Software is exempt from export
332 controls, regardless of its purpose.

333 As pointed out by the official US BIS guidance²⁸, the changes to the rules on
334 2021-Mar-29²⁹ have eliminated the e-mail notification requirement for ‘publicly
335 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>

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

²⁸<https://www.bis.doc.gov/index.php/policy-guidance/encryption>

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

336 software implementing “non-standard cryptography”³⁰, defined as any imple-
337 mentation of “cryptography” involving the incorporation or use of proprietary
338 or unpublished cryptographic functionality, including encryption algorithms or
339 protocols that have not been adopted or approved by a duly recognized inter-
340 national standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, and
341 GSMA) and have not otherwise been published.

342 Accordingly to the Linux Foundation, this removes the notification requirements
343 for most products based on OSS projects³¹.

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

349 Sample export control compliance vendor process

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

- 351 • **UC1:** Processing of ECCN classified packages/components in downstream
352 Apertis distributions for which an export notification has to be given to
353 legal authorities (e.g. 5D classified)
- 354 • **UC2:** Processing of ECCN classified packages/components in downstream
355 Apertis products for which an export notification has to be given to legal
356 authorities (e.g. 5D classified)
- 357 • **UC3:** Processing of ECCN classified packages/components in downstream
358 Apertis distributions for which an approval from legal authorities is re-
359 quired before getting exported (5E classified)
- 360 • **UC4:** Processing of ECCN classified packages/components in downstream
361 Apertis products for which an approval from legal authorities is required
362 before getting exported (5E classified)
- 363 • **UC5:** Handle changed ECCN classification of already added components
364 (5D to 5E, 5E to 5D, classified to unclassified, unclassified to classified) in
365 downstream Apertis distributions and products
- 366 • **UC6:** Handle SW components where the ECCN classification is different
367 for the binary and the source code

368 The basic requirements are:

- 369 1. Apertis and projects based on it have to handle SW components covered
370 under export control regulations
- 371 2. Some ECCN classified (5D) SW components require a listing of legal enti-
372 ties 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/>

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

382 ECCN numbers for SW components can be assumed as given, no detection

383 mechanism is needed.

384 Assessment questionnaire

385 The form below provides an example of the information that product teams need

386 to collect about their software components to decide whether a closer inspection

387 is needed or not, in case they need to be classified for export.

- 388 • **Producer**
- 389 *Emmett Brown SpA*
- 390 • **Name and version**
- 391 *Embedded Software for Flux Capacitor 42A*
- 392 • **Licenser (Vendor-contract partner)**
- 393 *End User*
- 394 • **Main function of the software**
- 395 *Operation of flux dispersal device Flux Capacitor 42A. The software is used*
- 396 *for data acquisition, signal processing and flux capacitance management.*
- 397 *Cryptography is used to protect the company IP, by encrypting and signing*
- 398 *the update files which can be installed by the user. Encryption/Singing is*
- 399 *also used to restrict the access to the operating system command line, used*
- 400 *for development and production.*
- 401 1. Central clearing over Software Consulting Service (SCS) (planned)?
- 402 Yes: Indication of PID
- 403 No
- 404 2. Indications concerning type of software
- 405 Licensed software
- 406 Freeware
- 407 Open Source Software (OSS)
- 408 Central Directive “Handling Open Source Software” is complied with:
- 409 Yes No
- 410 3. Are there indications concerning export control restrictions by the pro-
- 411 ducer/distributor/provider or in the license agreement?
- 412 Yes
- 413 Indication of Export Control List Number, ECCN, EAR99:

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

419 No

420 4. Supply by electronic media?

421 Yes

422 Indication of provision source and if so Internet link:

423 • <http://example.com/products/flux/src/>

424 No

425 5. Employment of cryptographic algorithms?

426 Yes

427 Indication of type of cryptography (symmetric/asymmetric) and key
428 length:

429 No

430 6. Which of the following functions/characteristics apply for the software?

431 Encryption for the protection of intellectual property and personal data
432 and not user-accessible (encryption / signing of update files)

433 Authentication function only (SSH login)

434 Mass-Market-Criteria

435 SSL / https

436 none

437 7. Has the software been applied or changed for military use?

438 Yes

439 No

440 8. Open Source Software [Only to be filled out in case of OSS as stand-alone
441 or integrated in products]

442 • Which kind of license applies for the OSS? Indication of license type
443 (e.g. GPL, CPL, MPL, LGPL):

444 – *Open SSH v7.9: BSD-Berkeley Software License Agreement, ISC,*
445 *BSD-2-Clause*

446 – *Open SSL v1.1.1: SSL-license, SSLeay License*

447 – *libcryptsetup12 v2.1.0: GLPv2 / LGPLv2*

448 – *libblockdev-crypto2 v2.20: LGPL-2.1+*

449 – *gnupg v1.4.7: GPL2.0+*

450 – *libcrypt20 v1.8.4: LGPLv2.1+*

451 – *krb5 v1.17: MIT*

452 – *nettle v3.2: LGPL-3.0+ or GPL-2.0+*

453 – *NSS v3.42: MPL 2.0*

454 – *P11-kit v0.23: BSD-3-Clause*

- 455 – *Cyrus-sasl2 v2.1.27: BSD 3 clause*
- 456 – *Libsecret v0.18.7: LGPLv2.1+*
- 457 – *Libsodium v1.017: ISC / BSD 2-clause / CC0 / MIT*
- 458 – *Volume-key v0.3.12: GPLv2*
- 459 – *Linux Kernel v4.19: GPLv2*
- 460 – *Shadow v4.5: BSD 2 / 3 clause / GPLv2.0+*
- 461 • Is the company required to provide the OSS as license term?
- 462 Yes
- 463 No
- 464 9. Which criteria apply concerning US-reexport legislation?
- 465 • Has the software been imported from the US/manufactured in the
- 466 US or is the producer/licensor a US-company?
- 467 Yes
- 468 No
- 469 • Has the software been produced based on listed US-software / US-
- 470 technology?
- 471 Yes
- 472 Indication of programming environment and export control list
- 473 number:
- 474 EAR99 ECCN 5D992 ECCN 5D002
- 475 No
- 476 • Result of assessment:
- 477 • List number:
- 478 – National:
- 479 – US Re-export control: EAR99 ECCN 5D992 ECCN 5D002
- 480 Direct product
- 481 – Date:
- 482 – ECO:

483 Purchased SW ECCN classification list

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

- 487 • SW component

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

- 488 • SW-Vendor address

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

- 489 • SW-Vendor contacts

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

- 490 • 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 the source)
source	30/01/2021	Italy

- 491 • Export Information

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

495 5E classified source and binary files in general are subject to authorization
496 **before** doing any export. After approval from the authorities, these 5E
497 files can be exported/enabled for access for the approved country and
498 legal entity. Especially if a 5E component is approved for export/access
499 to a country/legal entity, e.g. for development, and afterwards another
500 country or legal entity also needs to work with this 5E component, it also
501 has to be approved before using for development and other work. In some
502 situations, there may be an intermediate solution required to not block
503 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

- 504 • Vendor internal Software Subcontractormanagement

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

- 505 • Other

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

506 Approach

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

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

511 Each package can thus provide export control metadata such as ECCNs and
512 intended access controls: the metadata is associated to source and binary pack-
513 ages, no finer-grained granularity is in scope. Multiple ECCNs can be provided
514 since in some cases they need to change depending on how the final product is
515 distributed: for instance, software under 5D002 may need to be reclassified as
516 5D992 when distributed under the mass-market provisions.

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

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

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

526 Package metadata

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

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

535 The metadata shipped with each binary package will provide the following in-
536 formation:

- 537 • potentially applicable ECCNs
- 538 • for each ECCN, a short rationale for the categorization

- 539 • for 5D002 and 5D992, whether non-standard cryptography is also imple-
- 540 mented
- 541 • for restricted components, countries with access
- 542 • for restricted components, legal entities with access

543 **Software bill of materials**

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

- 547 • binary package name
- 548 • binary package version
- 549 • source package name
- 550 • source package version
- 551 • binary package ECCNs
 - 552 – for each ECCNs a rationale is provided
 - 553 – for 5D002 and 5D992, whether non-standard cryptography is also
 - 554 used
- 555 • link to binary package
- 556 • link to source
- 557 • countries with access
- 558 • legal entities with access

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

565 An hypothetical example of such metadata could be:

```
566 - purpose: Command line access during development
567   packages: [ openssh-server ]
568   non-standard-cryptography: false
569 - purpose: HTTPS connectivity for OTA updates and telemetry
570   packages: [ libssl1.1, libnettle8, libgnutls ]
571   non-standard-cryptography: false
572 - purpose: Software updates integrity and confidentiality
573   packages: [ libssl1.1 ]
574   non-standard-cryptography: false
575 - purpose: Device integrity
576   packages: [ "linux-image-*", libcryptsetup12 ]
577   non-standard-cryptography: false
```

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

580 Access control and audit

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

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

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

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

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

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