



License-compliant TLS stack for Apertis targets

1	Contents	
2	Goals and requirements	2
3	TLS stack pre v2021	3
4	TLS stack post v2022	3
5	GnuTLS	4
6	OpenSSL	4
7	NSS	5
8	Approach	6
9	Summary	6
10	TLS stack pre v2022	6
11	TLS stack post v2022	6

12 The Apertis distribution provides both a development environment for electronic
13 devices as well as a software stack to be used on them. In line with this goal,
14 the Apertis project strives to provide software components that, where there is
15 intent that they form part of the software stack on the devices themselves, are
16 free from licensing constraints that may make it unsuitable in certain use cases.
17 An example is software licensed under the terms of the GNU [GPL-3](https://www.gnu.org/licenses/gpl-3.0.en.html)¹ (General
18 Public License) or [LGPL-3](https://www.gnu.org/licenses/lgpl-3.0.en.html)² (Lesser General Public License) which are known
19 to present a problem as they sometimes [conflict with regulatory requirements](https://martyn.pages.apertis.org/apertis-website/policies/license-expectations/#licensing-constraints)³
20 and thus Apertis will take measures to avoid such packages being provided as
21 part of the “target” [package repositories](https://martyn.pages.apertis.org/apertis-website/policies/license-expectations/#apertis-repository-component-specific-rules)⁴.

22 Goals and requirements

23 The goal here is to provide TLS functionality not just for the packages contained
24 within its own repositories, but to support applications added by those utilizing
25 Apertis as well.

- 26 • **Requirement:** TLS implementation does not require code covered by
27 licenses that are incompatible with the target repositories rules
- 28 • **Requirement:** TLS implementation is licensed under terms that does
29 not preclude its use from existing target applications
- 30 • **Requirement:** TLS implementation is licensed under terms that does
31 not preclude its use from users proprietary applications

¹<https://www.gnu.org/licenses/gpl-3.0.en.html>
²<https://www.gnu.org/licenses/lgpl-3.0.en.html>
³[https://martyn.pages.apertis.org/apertis-website/policies/license-expectations/
#licensing-constraints](https://martyn.pages.apertis.org/apertis-website/policies/license-expectations/#licensing-constraints)
⁴[https://martyn.pages.apertis.org/apertis-website/policies/license-expectations/#apertis-
repository-component-specific-rules](https://martyn.pages.apertis.org/apertis-website/policies/license-expectations/#apertis-repository-component-specific-rules)

32 Given the security sensitive nature of the TLS stack, utilizing unmaintained soft-
33 ware here would be best avoided. Putting maintenance aside, these versions of
34 their respective TLS implementations may not be gaining support for any new
35 ciphers and TLS protocol versions, which will severely limit their usefulness as
36 time progresses. As well as not gaining newer protocol versions, the libraries
37 may not be updated to reflect the frequently changing [recommendations regard-](#)
38 [ing minimal protocol versions](#)⁵ that should be supported, which may result in
39 issues when attempting to access sites following the “Modern” recommendation.
40 Additionally, it is likely that newer versions of the packages utilizing these TLS
41 implementations will begin to require functionality added to newer versions of
42 the TLS libraries thus reducing the ability of Apertis to upgrade to these too.

43 TLS stack pre v2021

44 The “target” section of Apertis ships a variety of packages which use TLS from
45 a provided library. There are a number of software libraries that provide compet-
46 ing TLS implementations and which are provided under various licensing
47 terms. However, these projects do not always provide the same programming
48 interfaces, thus do not provide a drop in replacement for each other. Whilst
49 some users of TLS libraries may provide some level of abstraction to support
50 more than one TLS library, others may support only one and thus Apertis
51 currently provides [GnuTLS](#)⁶, [OpenSSL](#)⁷ and [NSS](#)⁸.

- 52 • **GnuTLS:** Apertis currently provides GnuTLS version 3.4.10. This is
53 an approximately four-year-old version of GnuTLS as shipped in Ubuntu
54 Xenial and thus is currently supported by Ubuntu and is expected to
55 be until 2022. GnuTLS is used directly or indirectly via libcurl in just
56 more than a dozen packages in target. Debian Buster, the current main
57 upstream of Apertis, includes a newer version of GnuTLS (currently 3.6.7)
58 though upgrading to this has already been avoided due to licensing issues
59 that will be discussed below.
- 60 • **OpenSSL:** Apertis currently provides OpenSSL version 1.1.1. This is
61 a relatively recent release in the 1.1.1 series and is packaged as part of
62 Debian Buster. The 1.1.1 series is [currently supported](#)⁹ as an LTS release
63 by the OpenSSL project until September 2023. Support for Debian Buster
64 [is expected](#)¹⁰ until June 2024.
- 65 • **NSS:** Apertis currently provides NSS version 3.42.1. This version is ap-
66 proximately a year and a half old, and is packaged as part of Debian

⁵https://wiki.mozilla.org/Security/Server_Side_TLS

⁶<https://www.gnutls.org/>

⁷<https://www.openssl.org/>

⁸<https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS>

⁹<https://www.openssl.org/policies/releasestrat.html>

¹⁰<https://wiki.debian.org/LTS>

67 Buster. As with OpenSSL, support for Debian Buster is expected until
68 June 2024.

69 Some of the packages requiring TLS support only support one of the currently
70 provided TLS implementations, often due to licensing compatibility. Other
71 packages, most notably libraries, support multiple TLS backends, frequently
72 including both GnuTLS and OpenSSL as options.

73 TLS stack post v2022

74 In order to have up to date libraries, specially TLS ones which very important
75 for security reasons Apertis based them on Debian as covered in the [Apertis
76 Release Flow](#)¹¹ which present the following issues for Apertis

77 GnuTLS

78 Whilst GnuTLS is licensed under the [LGPL-2.1](#)¹², it uses [Nettle](#)¹³ and [GMP](#)¹⁴.
79 Newer versions of both of these dependencies are now licensed as dual GPL-2
80 and LGPL-3, rather than LGPL-2.1.

81 To avoid including GnuTLS under LGPL-3 terms, should Apertis integrate a
82 newer version it would need to be utilized under the GPL-2 terms. This would
83 result in the binary GnuTLS library effectively being used under the terms of
84 the GPL-2 rather than LGPL-2.1. This would restrict Apertis users from using
85 this Apertis provided TLS implementation either directly or indirectly from any
86 non-GPL-2 compatible applications they wish to integrate into their systems, for
87 example in proprietary applications, where it would have the effect of requiring
88 the app to also be GPL-2 licensed.

89 In such a scenario, a newer GnuTLS library could be allowed by accepting its
90 dependencies under the GPL-2 license and restricting its use to places where
91 this license wouldn't be problematic, such as existing GPL-2 software. As the
92 existing applications written exclusively to use GnuTLS are GPL-2 or tolerant
93 of GPL-2, this is viable.

94 OpenSSL

95 The currently used version of OpenSSL is licensed under a custom GPL-
96 incompatible license. OpenSSL 3.0 (the next major version of OpenSSL)
97 will be licensed under the [Apache 2.0](#)¹⁵ license, which is compatible with the
98 GPL-3, but not GPL-2. This means that GPL-2 tools like `tumbler`, `connman`, `apt`

¹¹<https://martyn.pages.apertis.org/apertis-website/policies/release-flow/#apertis-release-flow>

¹²<https://www.gnu.org/licenses/old-licenses/lgpl-2.1.en.html>

¹³<https://www.lysator.liu.se/~nisse/nettle/nettle.html>

¹⁴<https://gmplib.org/>

¹⁵<https://www.apache.org/licenses/LICENSE-2.0>

99 or `systemd-journal-remote` cannot use the newer versions of OpenSSL without
100 effectively becoming GPL-3 licensed or through these upstream projects
101 applying a license exceptions (for example as [OpenVPN](#)¹⁶ has). The OpenSSL
102 project do not seem to hold a strong opinion on the compatibility, though
103 [suggest](#)¹⁷ either not using the GPL or applying an exception should you wish
104 to gain some legal certainty.

105 The compatibility between the current OpenSSL licensing and GPL-2 is based
106 on the premise that:

- 107 1. The [OpenSSL license](#)¹⁸ contains licensing terms not in the GPL (such as
108 the need to mention use of the software in all advertising material and
109 derivatives not being able to be called OpenSSL).
- 110 2. Linking OpenSSL with a GPL-2 application creates a derivative work
111 formed from the two pieces of code.
- 112 3. The GPL expressly [states](#)¹⁹ that one can't "impose any further restrictions
113 on the recipients' exercise of the rights granted herein" to the GPL licensed
114 work.

115 Likewise, the Apache 2.0 license, to which version 3 of OpenSSL will be release
116 under, contains clauses such as its [patent litigation license termination clause](#)²⁰.

117 While the argument made in step (2) is widely held by many, others disagree
118 with this interpretation, especially when the library is dynamically linked to
119 the application. For instance, it might be [claimed](#)²¹ that a dynamically linked
120 library is only truly combined with the application when run, not when dis-
121 tributed, so it would only become a derivative at that point, or it [might be](#)
122 [claimed](#)²² as this is the intended interface for interacting with a library this is
123 excluded either due to fair use laws in some jurisdictions or explicitly allowed
124 by the GPL when it [states](#)²³ "the act of running the Program is not restricted".

125 A further argument is that the GPL [states](#)²⁴ "as a special exception, the source
126 code distributed need not include anything that is normally distributed (in either
127 source or binary form) with the major components (compiler, kernel, and so on)
128 of the operating system on which the executable runs, unless that component
129 itself accompanies the executable". If the library is distributed as part of the
130 OS and can be considered a major component of it, then this clause doesn't
131 require the library to be considered as part of the software and therefore falls
132 outside of the scope of the license. A counter argument to this is that because
133 the application may also be considered to be distributed as part of the operating

¹⁶<https://spdx.org/licenses/openvpn-openssl-exception.html>

¹⁷<https://www.openssl.org/docs/faq.html#LEGAL2>

¹⁸<https://www.openssl.org/source/license-openssl-ssleay.txt>

¹⁹<https://www.gnu.org/licenses/old-licenses/gpl-2.0.html#section6>

²⁰<http://www.apache.org/licenses/LICENSE-2.0#patent>

²¹<https://lwn.net/Articles/548216/>

²²<https://www.linuxjournal.com/article/6366>

²³<https://www.gnu.org/licenses/old-licenses/gpl-2.0.html#section0>

²⁴<https://www.gnu.org/licenses/old-licenses/gpl-2.0.html#section3>

134 system this exception doesn't apply especially in embedded devices where the
135 software is distributed preinstalled as a complete entity.

136 Most distributions seem to either ignore this potential issue or do not consider a
137 policy to be needed. The Fedora project have deemed OpenSSL to be a [system
138 library](#)²⁵ as defined by the GPL and thus there is no incompatibility. Debian
139 historically decided that a linked library creates a derivative work and all the
140 packages it ships should be considered a combined work, though the decision
141 has [recently been taken](#)²⁶ to follow Fedora's lead here.

142 NSS

143 [Network Security Services](#)²⁷ (NSS) is a set of security libraries developed by
144 Mozilla. NSS provides its own API, which is currently only supported by a few
145 of the applications which use TLS in Apertis. It is licensed as [MPL-2.0](#)²⁸.

146 Approach

147 In order to fulfill the requirements the approach taken has been to upgrade
148 GnuTLS to a new version for those applications that can use it licensed as GPL-
149 2. With OpenSSL upgraded and retained as a system library, utilizing it, inline
150 with the approach taken by other distributions that have documented a specific
151 policy covering this.

152 The one outlier is the printing support in GTK which uses GnuTLS and which
153 potentially ends up causing GPL-2 dependencies in GTK. Whilst Debian have
154 also declared CUPS as a system library, we feel that the differing use cases for
155 Debian and Apertis make this less of a realistic position to take. We have there-
156 fore dropped printing support from GTK in order to remove this dependency
157 as we don't feel that this functionality is critical to Apertis' aim.

158 Summary

159 The tables below summarize the use of TLS libraries in various releases of Aper-
160 tis target images. We would expect proprietary applications to either utilize the
161 OpenSSL or NSS libraries as deemed appropriate by the individual projects.

162 TLS stack pre v2022

²⁵https://fedoraproject.org/wiki/Licensing:FAQ?rd=Licensing/FAQ#What.27s_the_deal_with_the_OpenSSL_license.3F

²⁶<https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=924937#105>

²⁷<https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS>

²⁸<https://www.mozilla.org/en-US/MPL/2.0/>

Component	License	OpenSSL	GnuTLS	Notes
apt	GPL-2+		X	
connman	GPL-2		X	
curl	curl and BSD-3-Clause and BSD-4-Clause-UC and ISC	X	X	also produ
glib-networking	LGPL-2.1+ and LGPL-2.1+ with OpenSSL exception		X	
liboauth	Expat/MIT		curl	
libmicrohttpd	LGPL-2.1+		X	uses curl f
neon27	LGPL-2.1+	X	X	
openjpeg	BSD-2		curl	
openldap	OLDAP-2.8		X	
rtmpdump	GPL-2+ (tools), LGPL-2.1+ (library)		X	
systemd	LGPL-2.1+ and GPL-2[+] and PD X		curl	
tumbler	LGPL-2.1+ and GPL-2+		curl	

163 **TLS stack post v2022**

Component	License	OpenSSL	GnuTLS	Notes
apt	GPL-2+		X	
connman	GPL-2		X	
curl	curl and BSD-3-Clause and BSD-4-Clause-UC and ISC	X	X	also produ after rebas
glib-networking	LGPL-2.1+ and LGPL-2.1+ with OpenSSL exception	X		
liboauth	Expat/MIT	curl		
libmicrohttpd	LGPL-2.1+		X	removed s
neon27	LGPL-2.1+	X	X	
openjpeg	BSD-2	curl		package li
openldap	OLDAP-2.8	X		
rtmpdump	GPL-2+ (tools), LGPL-2.1+ (library)		X	removed s
systemd	LGPL-2.1+ and GPL-2[+] and PD X	curl		package sy
tumbler	LGPL-2.1+ and GPL-2+	curl		