

Keywords	Commit ID	Comments	TD	Files changed	Commit i - 1
Technical debt					
debt					
may cause problem	9c478f202c152122e1588ecb15fc777c264d413c	When a certificate request is read in keep a copy of the - original encoding of the signed data and use it when outputing - again. Signatures then use the original encoding rather than - a decoded, encoded version which may cause problems if the - request is improperly encoded. was removed from ChangeLog	N		
	e9eff5016a4ec2153c037c1b888acd2755965755	The above comment was added to ChangeLog file	N		
workaround for bug					
hack/hacky/hackery	38c577d7587cac4b305dfa913029d9b750445700	* SUS. Use the same hack as OS X and FreeBSD use to work around on AIX, + * Solaris, and HPUX.	Y	include/compat/string.h libtls-standalone/include/string.h	
	5d8a1cf7155130bd8101090d7e1d0c2f90d9b123	/* Some functions historically defined in string.h were placed in strings.h by + * SUS. Use the same hack as OS X and FreeBSD use to work around on Solaris and HPUX. + */ was added to include/compat/string.h [NF] and removed from include/string.h[DF]	Y		
	df703ada9ff36dfa588d4a1eb19f9c18cd39afda	There are more pieces required to support building and using OpenSSL + with libtls, but this is an initial start at providing an + independent package for people to start hacking on. was added to ChangeLog	N		
	28353c1df15c3d0482a10ffe33fa34c053af2c2e	/* Some functions historically defined in string.h were placed in strings.h by + * SUS. Use the same hack as OS X and FreeBSD use to work around on Solaris and HPUX. + */ was added to libtls-standalone/include/string.h[NF]	N		
	51bfd4921a18552b72ecc15f282e52116c136554	This is mostly being used for generation of certificate requests. +## +## hacked by iang to do DSA certs - Server was added to tests/openssl.cnf	?		

	a91d1013cfb08ae17136f5ee412f5fb670199834	SUS. Use the same hack as OS X and FreeBSD use to work around on Solaris and HP-UX. was modified in include/string.h	Y		
	9c478f202c152122e1588ecb15fc777c264d413c	<p>This will allow some of the algorithm specific hackery</p> <ul style="list-style-type: none"> - needed to use the correct OID to be removed. was removed. 2) This hack will never - appear in 0.9.8 or later. was removed <p>3) [Massimiliano Pala <madwolf@hackmasters.net>] was removed 4) Clean old EAY MD5 hack from e_os.h. was removed 5) This is a simple way</p> <ul style="list-style-type: none"> - to bypass the X509_STORE hackery necessary to make this - work and makes it possible to use more efficient techniques - in future. was removed. 6) This is currently kind of a hack, and the perl code in objects.pl - isn't very elegant, but it works as I intended. was removed 7) New functionality allows removal of S/MIME code RC2 hack. was removed. 8) The primary motivation for this change is to avoid the same fiasco - that dogs private keys: there are several incompatible private key - formats some of which are standard and some OpenSSL specific and - require various evil hacks to allow partial transparent handling and - even then it doesn't work with DER formats. was removed from CHangeLog [DF] 	N		
	2b6dbc39ef274d5298daad1ff864be8fc3c56537	<p>/* Some functions historically defined in string.h were placed in strings.h by</p> <p>+ * SUS. Use the same hack as OS X and FreeBSD use to work around on Solaris.</p> <p>+ */ was added to include/string.h[NF]</p>	Y		
	e9eff5016a4ec2153c037c1b888acd2755965755	The comments appearing in 9c478f202c152122e1588ecb15fc777c264d413c were added to COPYING	N		
temporary solution					
this is wrong					
something bad is going on					
this indicates a more fundamental problem					

something serious is wrong					
doubt that this would work					
risk of this blowing up					
remove this code					
remove me					
remove me before production					
it doesn't work yet					
doesn't work yet					
Fix later					
revise later					
redo later					
reframe later					
redesign later					
save for later					
Fix in the future					
revise in the future					
save for the future					
redo in the future					
reframe in the future					
redesign in the future					

is problematic	9c478f202c152122e1588ecb15fc777c264d413c	This option is to allow - use of the new ASN1 code on platforms where exporting structures - is problematical (for example in shared libraries) but exporting - functions returning pointers to structures is not. was removed from ChangeLog file	N		
	e9eff5016a4ec2153c037c1b888acd2755965755	The above comment was added to ChangeLog	N		
causes issue					
cause for issue					
this can be a mess					
this is temporary and will go away					
hope everything will work					
workaround	a6d5b322762107cb4892dd66c83a427e99a13929	Removed workarounds for TLS client padding bugs. and Removed IE 6 SSLv3 workarounds. were added to ChangeLog	N		
	8414df69bc5463e13d91b865d8f21c294e2fe18b	Removed workarounds for obsolete SSL implementations was added to ChangeLog	N		
	2753f5ca876a909deec9f52404bd72c85ee625ca	Clang needs some workarounds, check for it was removed	?		
	5cf05de18ce848d7579f235758160ee12fcd85a5	The above comment was added	?		
	2c5ac47db473503689bec13671b1c5e67133ac33	Dead and disabled code removal including MD5, Netscape workarounds, + non-POSIX IO, SCTP, RFC 3779 support, many #if 0 sections, and more. was added to ChangeLog	N		
	20e329e2720343b2ec4c320d8ec6e77dc8e63aee	Removed nonfunctional Netscape browser-hang workaround code. was added to ChangeLog	N		

		<p>Workaround for the "TLS hang bug" (see FAQ and PR#2771): if the</p> <ul style="list-style-type: none"> - TLS client Hello record length value would otherwise be > 255 and - less than 512 padded with a dummy extension containing zeroes so it - is at least 512 bytes long. was removed. <p>2) As a workaround use the maximum permitted</p> <ul style="list-style-type: none"> - client version in client hello, this should keep such servers happy - and still work with previous versions of OpenSSL. was removed <p>3) Disable code workaround for ancient and obsolete Netscape browsers</p> <ul style="list-style-type: none"> - and servers: an attacker can use it in a ciphersuite downgrade attack. was removed <p>4) WARNING: applications which</p> <ul style="list-style-type: none"> - included workarounds for the old buggy behaviour will need to be modified - or they could free up already freed BIOs. was removed. <p>5) Disable code workaround for ancient and obsolete Netscape browsers</p> <ul style="list-style-type: none"> - and servers: an attacker can use it in a ciphersuite downgrade attack. was removed. <p>6) On some versions of WIN32 Heap32Next is very slow. This can cause</p> <ul style="list-style-type: none"> - excessive delays in the RAND_poll(): over a minute. As a workaround - include a time check in the inner Heap32Next loop too. was removed. <p>7) X509 verify fixes. Disable broken certificate workarounds when</p> <ul style="list-style-type: none"> - X509_V_FLAGS_X509_STRICT is set. was removed and many other such comments were removed from ChangeLog 	N		
	9c478f202c152122e1588ecb15fc777c264d413c				
	e9eff5016a4ec2153c037c1b888acd2755965755	The above comments were added to ChangeLog	N		
can cause problems					
may cause problems	9c478f202c152122e1588ecb15fc777c264d413c	Same as may cause problem			
	e9eff5016a4ec2153c037c1b888acd2755965755	Same as may cause problem			
this is temporary					
problem will go away					
in the future	4a931b58fc6c9a20e37841140019032f4536a0ba	<p>The Operating System including object format, if it has switched</p> <p>+ # to ELF recently, or will in the future.</p>	N		

	9c478f202c152122e1588ecb15fc777c264d413c	<p>Some</p> <ul style="list-style-type: none"> - time in the future, des_old.h and the libdes compatibility functions - will be disable (i.e. OPENSSL_DISABLE_OLD_DES_SUPPORT will be the default), and then completely removed. <p>was removed from ChangeLog. 2) removed obsolete files (the test scripts will be replaced</p> <ul style="list-style-type: none"> - by better Test::Harness variants in the future) was removed from ChangeLog 	N		
	e9eff5016a4ec2153c037c1b888acd2755965755	<p>The comments " Some</p> <ul style="list-style-type: none"> + time in the future, des_old.h and the libdes compatibility functions + will be disable (i.e. OPENSSL_DISABLE_OLD_DES_SUPPORT will be the default), and then completely removed." and "removed obsolete files (the test scripts will be replaced + by better Test::Harness variants in the future)" were added to ChangeLog 	N		
will go away					
should be avoided					
TYPE1					
this isn't very solid					
don't use this					
get rid of this					
just abandon it					
fix this crap					
it doesn't work yet					
crap					

inconsistency	9c478f202c152122e1588ecb15fc777c264d413c	Rename openssl x509 option '-crext', which was added in 0.9.5, - to '-crext' (= clear extensions), as intended and documented. - [Bodo Moeller; inconsistency pointed out by Michael Attili - <attili@amaxo.com>] was removed from ChangeLog	N		
	e9eff5016a4ec2153c037c1b888acd2755965755	Rename openssl x509 option '-crext', which was added in 0.9.5, + to '-crext' (= clear extensions), as intended and documented. + [Bodo Moeller; inconsistency pointed out by Michael Attili + <attili@amaxo.com>] was added to ChangeLog	N		
take care					
something's gone wrong					
unknown why we ever experience this					
treat this as a soft error					
this isn't quite right					
trial and error					
this doesn't look right					
is this line really safe					
impact of the past design					
impact of the past decision					
quick fix					
better scheme needed					
You have been warned					

a really bad idea					
-------------------	--	--	--	--	--