

Camellia Cipher Suites for TLS

<draft-kato-tls-rfc4132bis-00.txt>

Akihiro KATO

IETF 71th March 2008

TLS Working Group



Back Ground

- ❁ RFC4132 Published July 2005
- ❁ Adapted several FOSS
 - OpenSSL 0.9.8c or later
 - GnuTLS
 - Firefox3
 - IPsec Stack (Linux, FreeBSD)



Connect to GnuTLS Test Server by

The screenshot shows a Mozilla Firefox 3 Beta 3 browser window with the address bar set to `https://test1.gnutls.org/`. The page content includes a lock icon and the text "This is Apache". A table of technical details is visible, and a "Page Info" window is open on the right, showing security information.

GNU TLS test site: test1.gnutls.org - Mozilla Firefox 3 Beta 3

File Edit View History Bookmarks Tools Help

`https://test1.gnutls.org/`

GNU TLS test site: test1.gnut...

This is **Apache**

Welcome vis

Library version:	GnuTLS/2.2.1
Interface version:	mod_gnutls/0.5.1
Session ID:	3F2DD3CA08462
Protocol version:	TLS1.0
Cipher suite:	DHE_RSA_CAME
Cipher key size:	256
Cipher export status:	false
Compression method:	NULL
Server Certificate Type:	X.509
Server DN:	C=GR,O=GnuTL:
Server's certificate serial:	4752842F
Server's certificate version:	3
Server's certificate activation time:	Dec 02 10:08:48
Server's certificate expiration time:	May 02 10:08:51
Server's certificate public key:	RSA
Server's certificate Signature algorithm:	RSA-SHA
Server's Issuer DN:	CN=GnuTLS tes
Client's version:	Mozilla/5.0 (Wind
Client's certificate verification status:	NONE

If your browser supports session resuming, then you should

If you always see the same certificate, no matter which ser

Indication.

About the servers:

Done

test1.gnutls.org

Page Info - https://test1.gnutls.org/

General Media Permissions **Security**

Web Site Identity

Web site: **test1.gnutls.org**
Owner: **GnuTLS**
Verified by: **GnuTLS test CA**

This web site provides a certificate to verify its identity. [View Certificate](#)

Privacy & History

Have I visited this web site before today? **No**

Is this web site storing information (cookies) on my computer? **No** [View Cookies](#)

Have I saved any passwords for this web site? **No** [View Saved Passwords](#)

Technical Details

Connection Encrypted: High-grade Encryption (Camellia-256 256 bit)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

Proposed New Cipher Suites

RSA_WITH_CAMELLIA_128_CBC_SHA256
DH_DSS_WITH_CAMELLIA_128_CBC_SHA256
DH_RSA_WITH_CAMELLIA_128_CBC_SHA256
DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256
DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
DHE_anon_WITH_CAMELLIA_128_CBC_SHA256

RSA_WITH_CAMELLIA_256_CBC_SHA384
DH_DSS_WITH_CAMELLIA_256_CBC_SHA384
DH_RSA_WITH_CAMELLIA_256_CBC_SHA384
DHE_DSS_WITH_CAMELLIA_256_CBC_SHA384
DHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
DHE_anon_WITH_CAMELLIA_256_CBC_SHA384

RSA_WITH_CAMELLIA_256_CBC_SHA512
DH_DSS_WITH_CAMELLIA_256_CBC_SHA512
DH_RSA_WITH_CAMELLIA_256_CBC_SHA512
DHE_DSS_WITH_CAMELLIA_256_CBC_SHA512
DHE_RSA_WITH_CAMELLIA_256_CBC_SHA512
DHE_anon_WITH_CAMELLIA_256_CBC_SHA512

RSA_WITH_CAMELLIA_128_CBC_SHA256
DH_DSS_WITH_CAMELLIA_128_CTR_SHA256
DH_RSA_WITH_CAMELLIA_128_CTR_SHA256
DHE_DSS_WITH_CAMELLIA_128_CTR_SHA256
DHE_RSA_WITH_CAMELLIA_128_CTR_SHA256
DHE_anon_WITH_CAMELLIA_128_CTR_SHA256

RSA_WITH_CAMELLIA_256_CTR_SHA384
DH_DSS_WITH_CAMELLIA_256_CTR_SHA384
DH_RSA_WITH_CAMELLIA_256_CTR_SHA384
DHE_DSS_WITH_CAMELLIA_256_CTR_SHA384
DHE_RSA_WITH_CAMELLIA_256_CTR_SHA384
DHE_anon_WITH_CAMELLIA_256_CTR_SHA384

RSA_WITH_CAMELLIA_256_CTR_SHA512
DH_DSS_WITH_CAMELLIA_256_CTR_SHA512
DH_RSA_WITH_CAMELLIA_256_CTR_SHA512
DHE_DSS_WITH_CAMELLIA_256_CTR_SHA512
DHE_RSA_WITH_CAMELLIA_256_CTR_SHA512
DHE_anon_WITH_CAMELLIA_256_CTR_SHA512



Issues and Questions

❁ Explosion of Cipher suites

- Eliminate CTR, SHA384 or SHA512
 - 36 New Cipher suites → 12 New Cipher suites

❁ SHA-384 vs. SHA512

- NIST SP 800-57 said “256bit security for HMAC are HMAC-256, HMAC-384, HMAC-512”
- TLS spec takes 384



What's Next?

- ❁ Shrink Cipher suites
- ❁ Take in comments
- ❁ Fix errors
- ❁ Submit A.S.A.P to I-D repository

Questions and comments?

