01.Find and document information for the Transport Layer Security (TLS) cryptographic.

Като цяло в Интернет има много информация за този протокол.Ще споделя някоя от тях и също така за по-любознателните ще кача различни сайтове които намерих.

**Cryptographic security protocols: TLS and SSL**

Cryptographic protocols provide secure connections, enabling two parties to communicate with privacy and data integrity. The Transport Layer Security (TLS) protocol evolved from that of the Secure Sockets Layer (SSL).

Applications use TLS or SSL to establish secure connections between two communicating parties. The primary goal of both protocols is to provide privacy and data integrity. Other goals are as follows:

* Enabling interoperability between applications
* Providing an extensible framework that can readily incorporate new public key and bulk encryption methods
* Ensuring relative computational efficiency

Both TLS and SSL comprise two layers: a Record Protocol and a Handshake Protocol.

Although the two protocols are similar, the differences are sufficiently significant that SSL 3.0 and the various versions of TLS do not interoperate.

<http://publib.boulder.ibm.com/infocenter/wmqv7/v7r0/index.jsp?topic=%2Fcom.ibm.mq.csqzas.doc%2Fsy10630_.htm>

**Transport Layer Security (TLS)**

TLS is an Internet Standard for providing data confidentiality. Along with the pages on [SASL (Simple Authentication and Security Layer)](http://www.isode.com/products/sasl.html) and [Strong Authentication](http://www.isode.com/products/strong-auth-inf.html), this page describes the infrastructure of the Isode products that use cryptography.

Transport Layer Security (TLS) is an Internet Standard for providing data confidentiality, and is used by Isode server products. TLS also provides strong authentication using X.509 (which is described [here](http://www.isode.com/products/strong-auth-inf.html)).

**Cryptographic Algorithms**

Isode TLS can use the following Cipher Suites:

|  |  |  |
| --- | --- | --- |
| **Cipher** | **Key Length (Standard)** | **Key Length (High Grade)** |
| DES | 40, 56 |  |
| Triple DES | not supported | 168 (112 effective) |
| AES | not supported | 128, 256 |
| RC4 | 40, 56 | 128 |
| RC2 | 40, 56 | 128 |

Where X.509 based authentication is used, the supported cryptographic are described in the [strong authentication product overview](http://www.isode.com/products/strong-auth-inf.html).

Diffie Hellman key exchange and SHA (Secure Hash Algorithm) may be used with Isode TLS, either in conjunction with X.509 based authentication or independently.

Configuration of Isode TLS will select valid combinations of Cipher Suite and Authentication. Valid combinations are documented in the Isode Manual.

**Standard and High Grade Encryption**

Isode's products support data encryption at up to 56 bits, as shown in column 2 of the table above.

High Grade versions of the Isode products are available, supporting the algorithms and key lengths shown in column 3 of the table above. Availability of these products is dependent on the country of end use, and controlled by UK Export regulations. Use in the European Union does not require an export license. Use in US, Canada, Australia, New Zealand, Japan, Switzerland and Norway is permitted under a standard export license. Use in all other countries requires an export license. Isode does not anticipate problems in obtaining an export license for reasonable use of the Isode products.

**Conformance**

Isode products conform to the following standards:

* RFC 2246: The TLS Protocol Version 1.0, T. Dierks, C. Allen, January 1999
* RFC 3268: Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)

**Underlying Technology**

Isode makes use of the OpenSSL package to provide TLS data confidentiality services. OpenSSL has FIPS 140-2 conformance which is a US government security standard for cryptographic modules defined [here](http://csrc.nist.gov/cryptval/140-2.htm).

This is a high quality package used by many commercial products. Isode would like to acknowledge the contribution from the authors of OpenSSL, and of the organizations that have funded work on these packages.

There is also a strong security benefit in using open source technology, particularly for the cryptographic components. Because the source is widely used and openly available, it has been subject to substantial peer review. This leads to a high confidence in the security of these products.

Isode tracks versions of OpenSSL, and in the event of security fixes to OpenSSL which may Impact Isode products, will release product updates.

**Isode's TLS Support**

Isode uses TLS in the following protocols and products:

* LDAP (in M-Vault)
* SMTP (in M-Switch)
* LMTP (in M-Switch)
* SOM Isode Protocol (in M-Switch)
* IMAP (in M-Box)
* POP3 (in M-Box)
* XMPP (in M-Link and the Swiften XMPP Client Library)

<http://www.isode.com/products/tls.html>

И още информация на:

<http://en.wikipedia.org/wiki/Transport_Layer_Security>

<http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS>

<http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb60-eng.html>