Transport Layer Security WG

IETF 71

Agenda

1. Agenda bashing (5 minutes) - chairs
    - Bluesheets
    - Agenda changes
    - Scribe for minutes
    - Jabber scribe
2. Document status (5 minutes) - chairs
    - Progress since last IETF
3. DTLS 1.2 (30 minutes) - Eric Rescorla
4. TLS Cert Cache (20 minutes) - Stefan Santesson
5. DTLS Mobi-D (20 minutes) - Michael G. Williams

Document Status (RFCs) (I)

The TLS Protocol Version 1.0	RFC 2246	Published
Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)	RFC 2712	Published
Upgrading to TLS Within HTTP/1.1	RFC 2817	Published
HTTP Over TLS	RFC 2818	Published
AES Ciphersuites for TLS	RFC 3268	Published
Transport Layer Security (TLS) Extensions	RFC 3546	Published
Transport Layer Security Protocol Compression Methods	RFC 3749	Published
Addition of Camellia Cipher Suites to Transport Layer Security (TLS)	RFC 4132	Published
Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)	RFC 4279	Published
The The Transport Layer Security (TLS) Protocol Version 1.1	RFC 4346	Published
Transport Layer Security (TLS) Extensions	RFC 4366	Published
Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)	RFC 4492	Published
Pre-Shared Key (PSK) Cipher Suites with NULL Encryption for Transport Layer Security (TLS)	RFC 4785	Published

Document Status (RFCs) (II)

Using OpenPGP keys for TLS authentication	RFC 5081	Published
Using the Secure Remote Password (SRP) Protocol for TLS Authentication	RFC 5054	Published
The Transport Layer Security (TLS) Protocol Version 1.2 (RFC 5246)	RFC 5246	Published
TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)	RFC 5289	Published
AES Galois Counter Mode (GCM) Cipher Suites for TLS	RFC 5288	Published
DES and IDEA Cipher Suites for Transport Layer Security (TLS)	RFC 5469	Published
Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode	RFC 5487	Published
ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)	RFC 5489	Published

Document Status (IDs)

Keying Material Exporters for Transport Layer Security (TLS)	draft-ietf-tls-extractor-05	**WGLC Finished**
Transport Layer Security (TLS) Extensions: Extension Definitions	draft-ietf-tls-rfc4366-bis-03	**Ready for WGLC**
Datagram Transport Layer Security version 1.2	draft-ietf-tls-rfc4347-bis-03	**Ready for WGLC**