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. TLS Extensions: Extension Definitions (10 minutes) - Don Eastlake
4. DES and IDEA Cipher Suites for Transport Layer Security (TLS) (10 minutes) - Pasi Eronen
5. ECDHE_PSK Ciphersuites for Transport Layer Security (TLS) (10 minutes) - Pascal Urien
6. DTLS 1.1 (10 minutes) - Eric Rescorla
7. Camellia Cipher Suites for TLS (10 minutes) - Akihiro Kato

Document Status (RFCs)

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
Using OpenPGP keys for TLS authentication	RFC 5081	Published
Using the Secure Remote Password (SRP) Protocol for TLS Authentication	RFC 5054	Published

Document Status (IDs)

The Transport Layer Security (TLS) Protocol Version 1.2	draft-ietf-tls-rfc-4346bis-09	**Approved**
TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode	draft-ietf-tls-ecc-new-mac-04	**WGLC Finished**
AES-GCM Cipher Suites for TLS	draft-ietf-tls-rsa-aes-gcm-02	**WGLC Finished**
Transport Layer Security (TLS) Extensions: Extension Definitions	draft-ietf-tls-rfc4366-bis-02	In progress
Keying Material Extractors for Transport Layer Security (TLS)	draft-ietf-tls-extractor-01	**New**
ECDHE_PSK Ciphersuites for Transport Layer Security (TLS)	draft-ietf-tls-ecdhe-psk-00	**New**
DES and IDEA Cipher Suites for Transport Layer Security (TLS)	draft-ietf-tls-idea-00	**New**