Session Key Interface (SKI) for TLS and DTLS

draft-cairns-tls-session-key-interface-01

K. Cairns, J. Mattsson, R. Skog, D. Migault

Architecture

```
+------------+  Handshake  +-------------+    SKI    +------------+
| TLS Client | <---------> | Edge Server | <-------> | Key Server |
+------------+             +-------------+           +------------+
```

- Edge Servers only host public material
- Key Server:
  - owns the private
  - performs the private key related operations

Key Server operations

1. RSA decryption when the TLS Client provides the encrypted pre_master in ClientKeyExchange message.
2. Sign EDH (with ClientHello.random and the ServerHello.random) in KeyExchange message.
   - RSA signature with DHE_RSA, ECDHE_RSA
   - ECDSA signature with ECDHE_ECDSA

Design Questions

1) Should we consider RSA as KeyExchangeAlgorithm?

2) What is the best design for a signing request:
    a. Provide the hash to the Key Server
        - Chosen plain text attack
    b. Provide all data to the Key Server
        - Additional bytes to be sent
    c. Enable both scheme, leave

3) (if RSA is considered similar consideration as 2) for master secret / extended master secret.

Next Steps

- Current version:
  - Security analysis of the architecture
  - Abstract description of SKI
- Next step:
  - Document with an abstract description
  - Document with an implementation HTTPS/JSON

Thank you!