

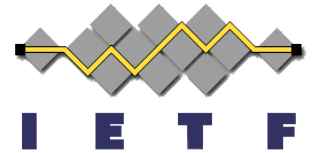
TLS Cached Information Extension

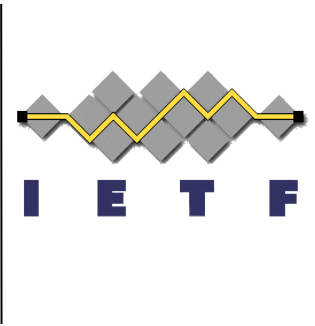
TLS WG

draft-ietf-tls-cached-info-13

IETF 86

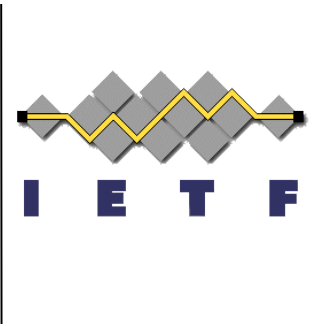
March, 2013





Current Approach

- Client indicates the support of the cached info extension.
 - Example: `cached_information=(certificate_chain)`
- Server returns the fingerprint instead of the complete info.
- Example:
 - `opaque ASN.1Cert<1..224-1>;`
 - `struct { ASN.1Cert certificate_list<0..224-1>; } Certificate;`
 - `struct { CachedObject cached_objects<1..224-1>; } Certificate;`



New Proposal

- Instead of sending the fingerprint just omit sending the object altogether.

Feedback?

