TLS – Cached Information

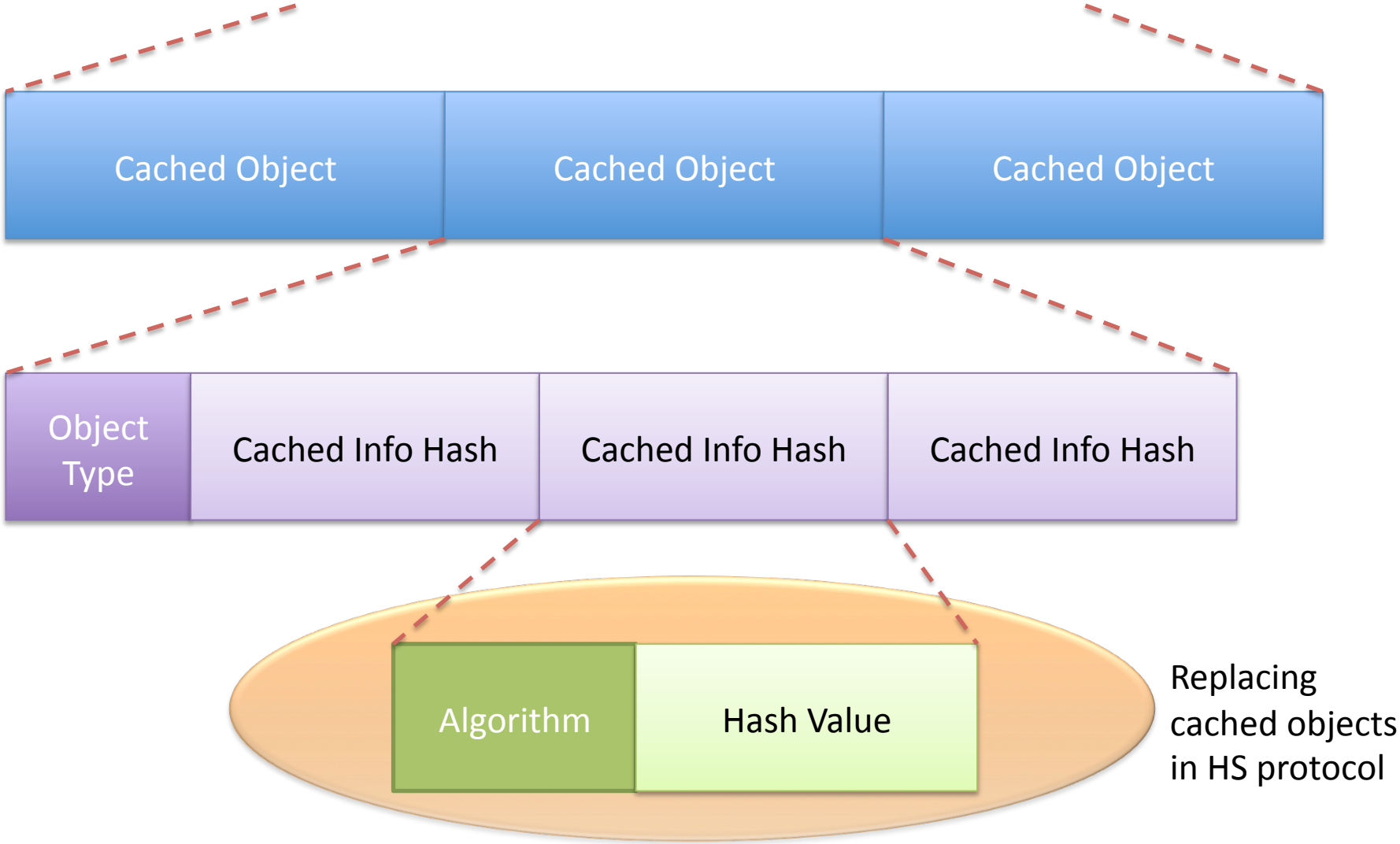
Stefan Santesson

AAA-sec.com

Approach

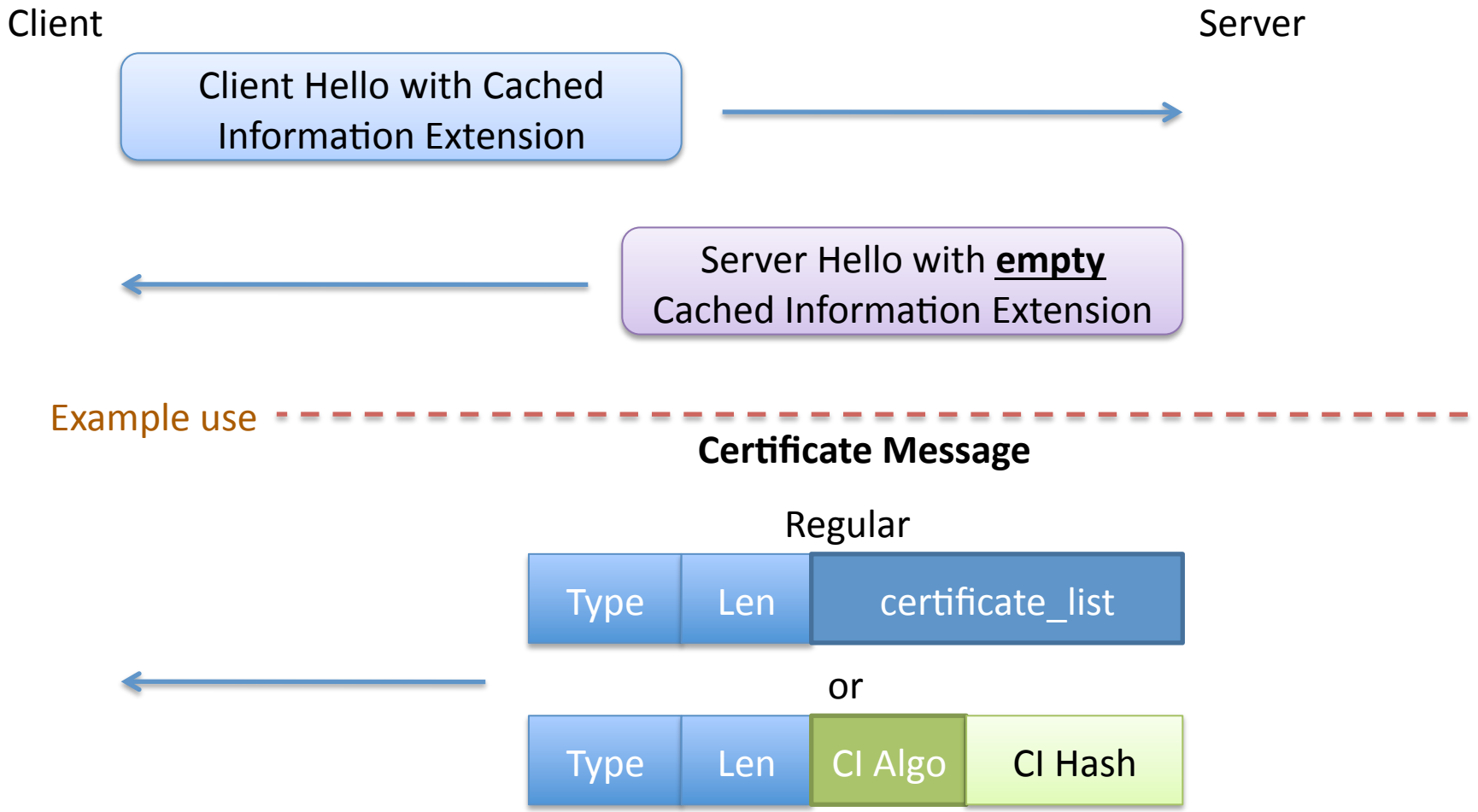
- Allows cached information to be omitted in handshake protocol
  1. Client provides hashes over cached data in Client Hello
  2. Server acknowledge in Server Hello
  3. Server replace cached info with hash supplied by client
- Finished message calculated over actual exchanged data

Cached Information



Replacing cached objects in HS protocol

Message flow



Status

- Last IETF indicated potential objections to the proposed approach, alt proposed improvements
  - Need for server to indicate in server hello exactly which objects it intends to replace
  - Server indication of accepted/preferred hash algorithms for further optimizations
- No concrete proposals since last IETF
- Thus - No changes since last IETF

Way forward

- Author Request to WG Last Call the document