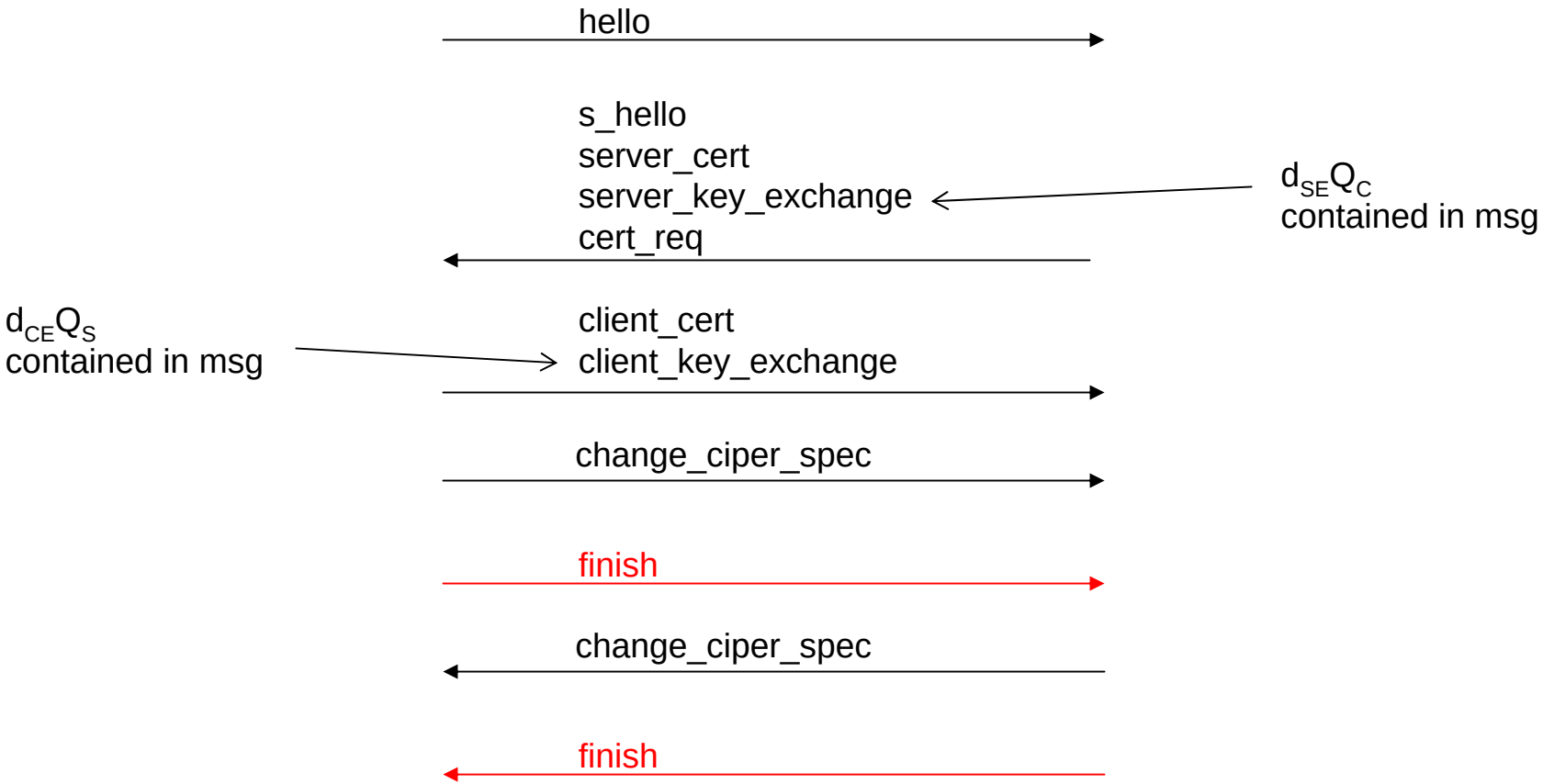
IEEE

Summary of Elliptic Curve Key Exchange in TLS

Working Group Discussion on 11/15/06
Notes by Guy Hutchison

EAP-TLS Message Exchange



Operations Required

- Random Number Generator (RNG)
- Sign (ec_sign)
  - uc_ansi_x9_p256r1 w/ SHA-256
- Verify (ec_verify)
  - Verify certificate path validation for each certificate in chain
  - Verify signed DHE parameters
- EC_sign
  - Sign the DHE parameters
- ECDH – point multiply

Primitives Required

- RNG
- Point multiplier (for EC)
- SHA hash calculator

Additional Notes

- The basic scheme is ECDHE_ECDSA: using ephemeral Diffie-Hellman key agreement with ECDSA signing certificate for mutual authentication.
  1. This discussion was based around RFC 4492.
  2. In the current concept for EC-based DevID credentials, the corresponding RFC 4492 elliptic curve identifier is secp256r1.
  3. We noted that an implementation would need both SHA-1 and SHA-256 at different points in the protocol.