Simple Keys for Simple Smart Objects

Carsten Bormann 2012-03-23
All the work was actually done by:
Stefanie Gerdes, Silke Schäfer,
Olaf Bergmann, Klaus Hartke

Simple

This is way too **complicated**. People have to **configure** this thing and then learn the **buttons** to press. This will **never** fly...

1994

SMS

Secure Bootstrapping of Nodes in a CoAP Network

- Try to get by with Symmetric PSK

All the work was actually done by:
Stefanie Gerdes, Silke Schäfer, Olaf Bergmann, Klaus Hartke

Insert legally unencumbered picture of penny-size device here.

- Don’t think Moore’s law will fix it!

Constrained nodes: orders of magnitude

10/100 vs. 50/250

- There is not just a single class of “constrained node”

- Class 0: too small to securely run on the Internet
  - “too constrained”
- Class 1: ~10 KiB data, ~100 KiB code
  - “quite constrained”, “10/100”
- Class 2: ~50 KiB data, ~250 KiB code
  - “not so constrained”, “50/250”

- These classes are not clear-cut, but may structure the discussion and help avoid talking at cross-purposes

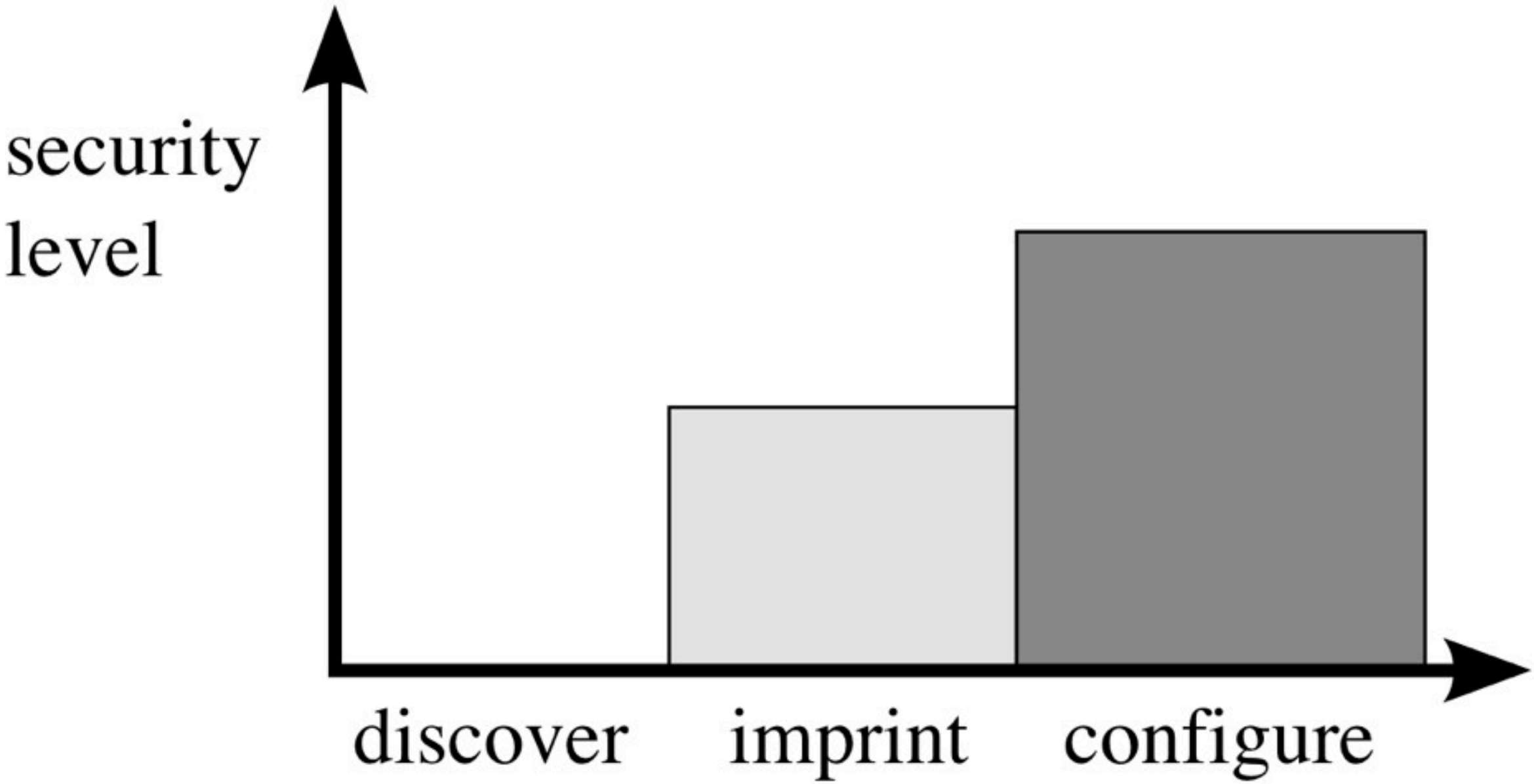


Fig. 2. Increasing security level along the bootstrapping process

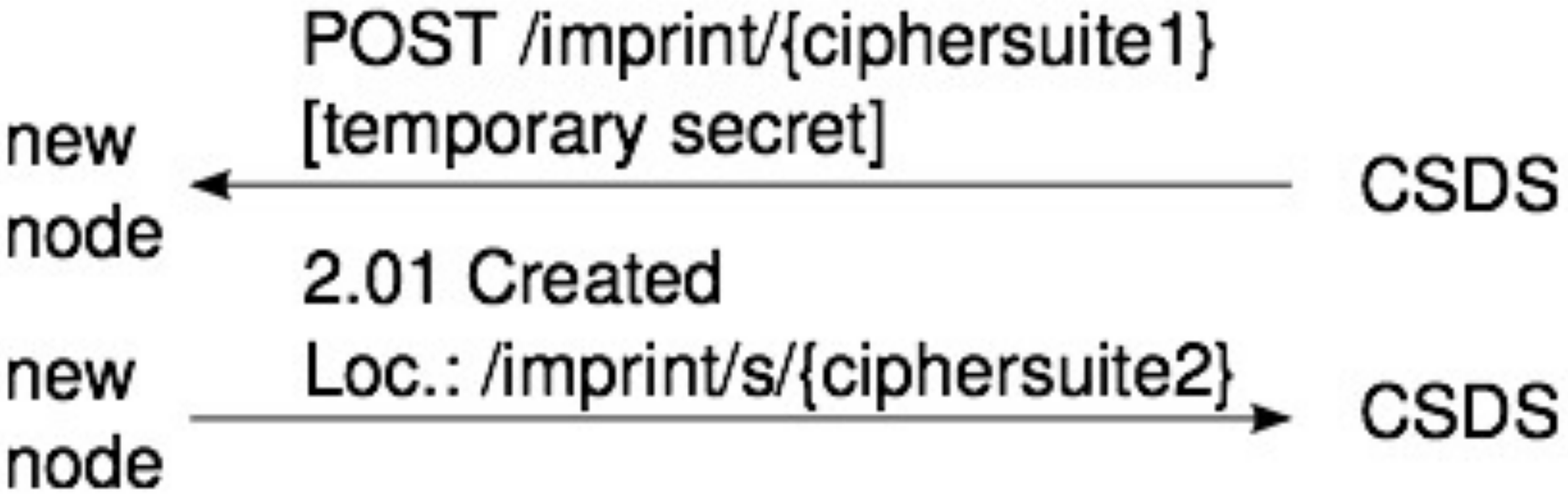


Fig. 4. Imprinting a temporary secret

CSDS = CoAP Service Discovery Server

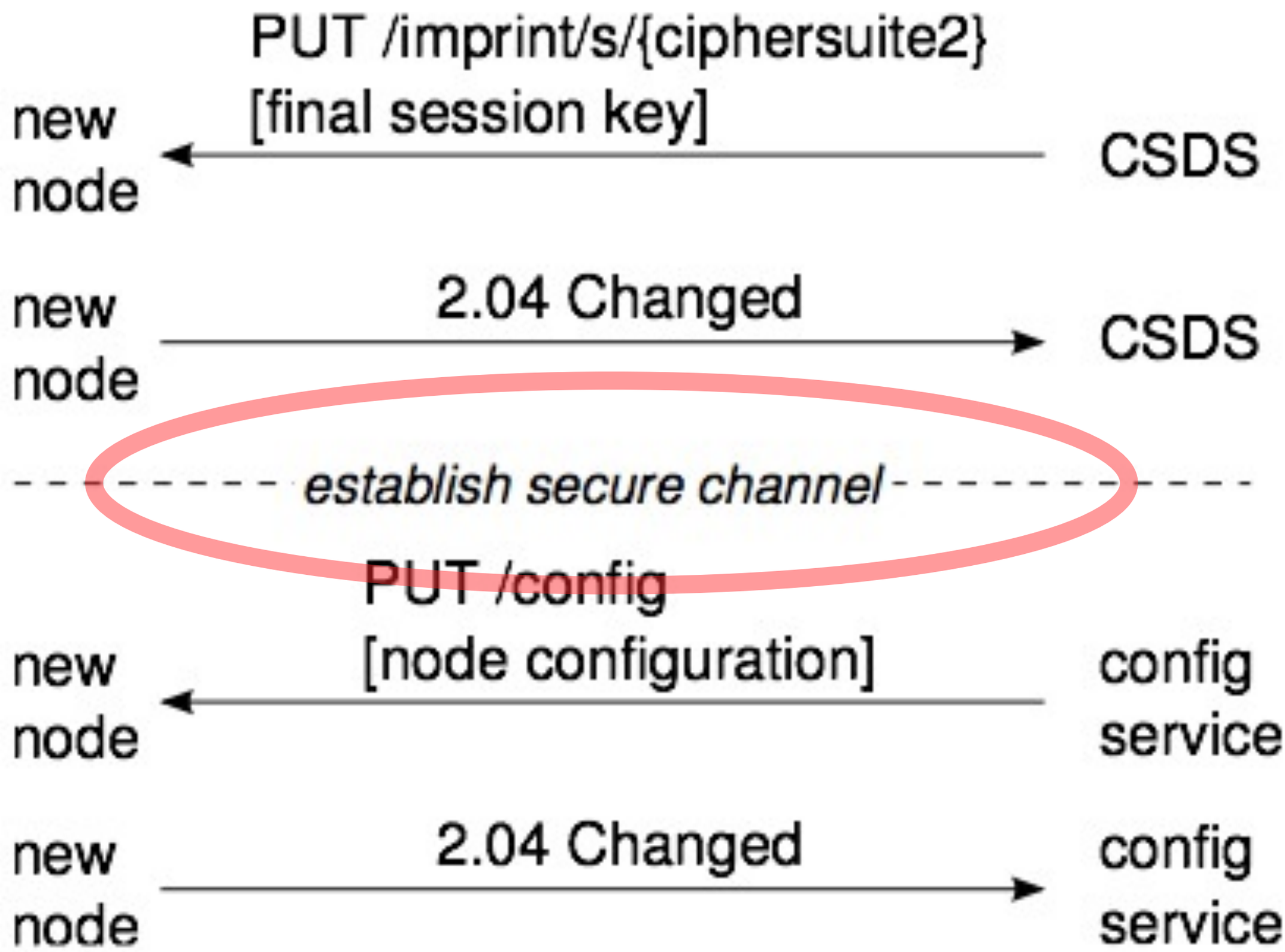


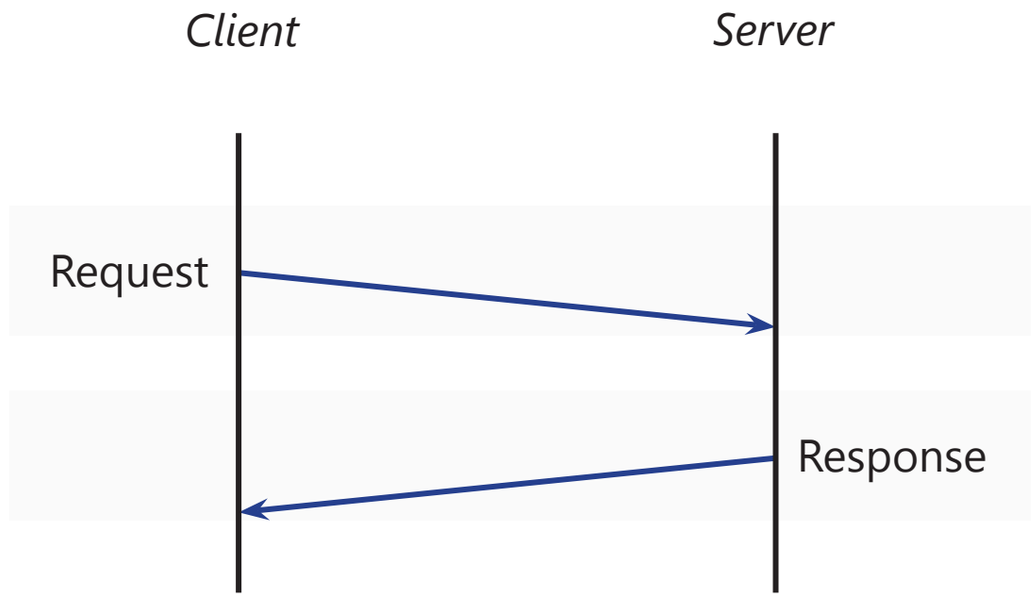
Fig. 5. Imprinting the final session key and configuring the new node

DTLS

Datagram TLS

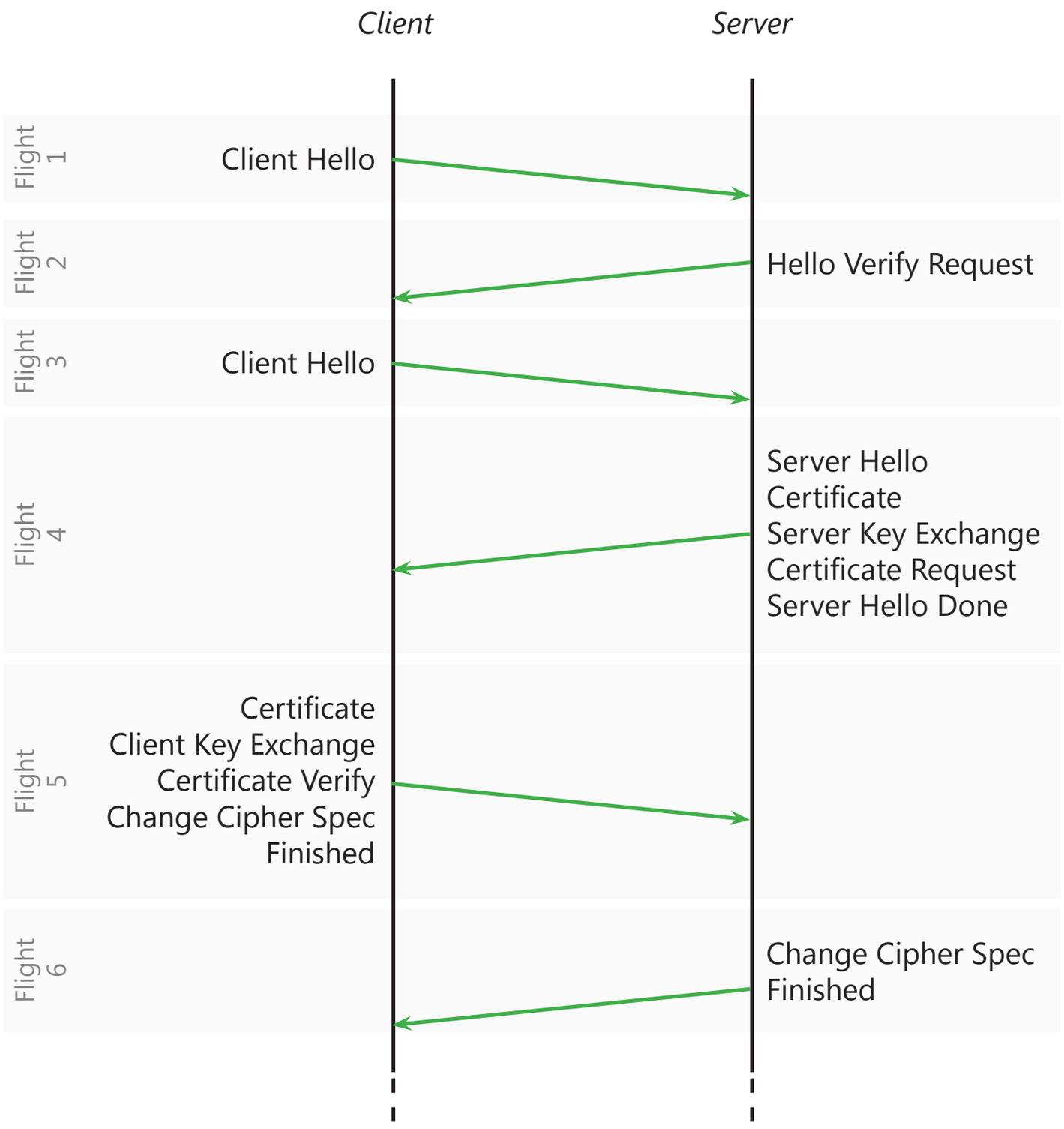
Datagram Transport Layer Security

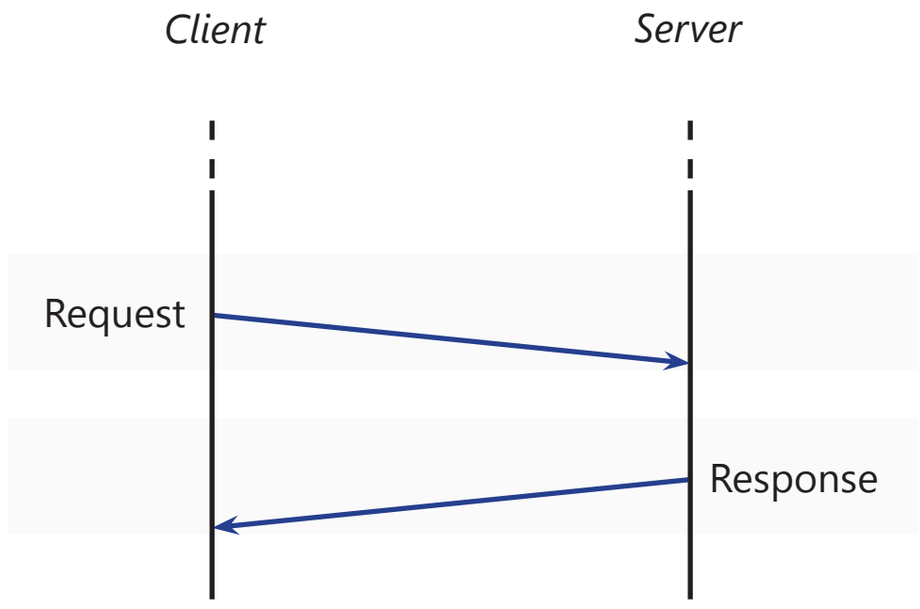
CoAP without DTLS



1 roundtrip

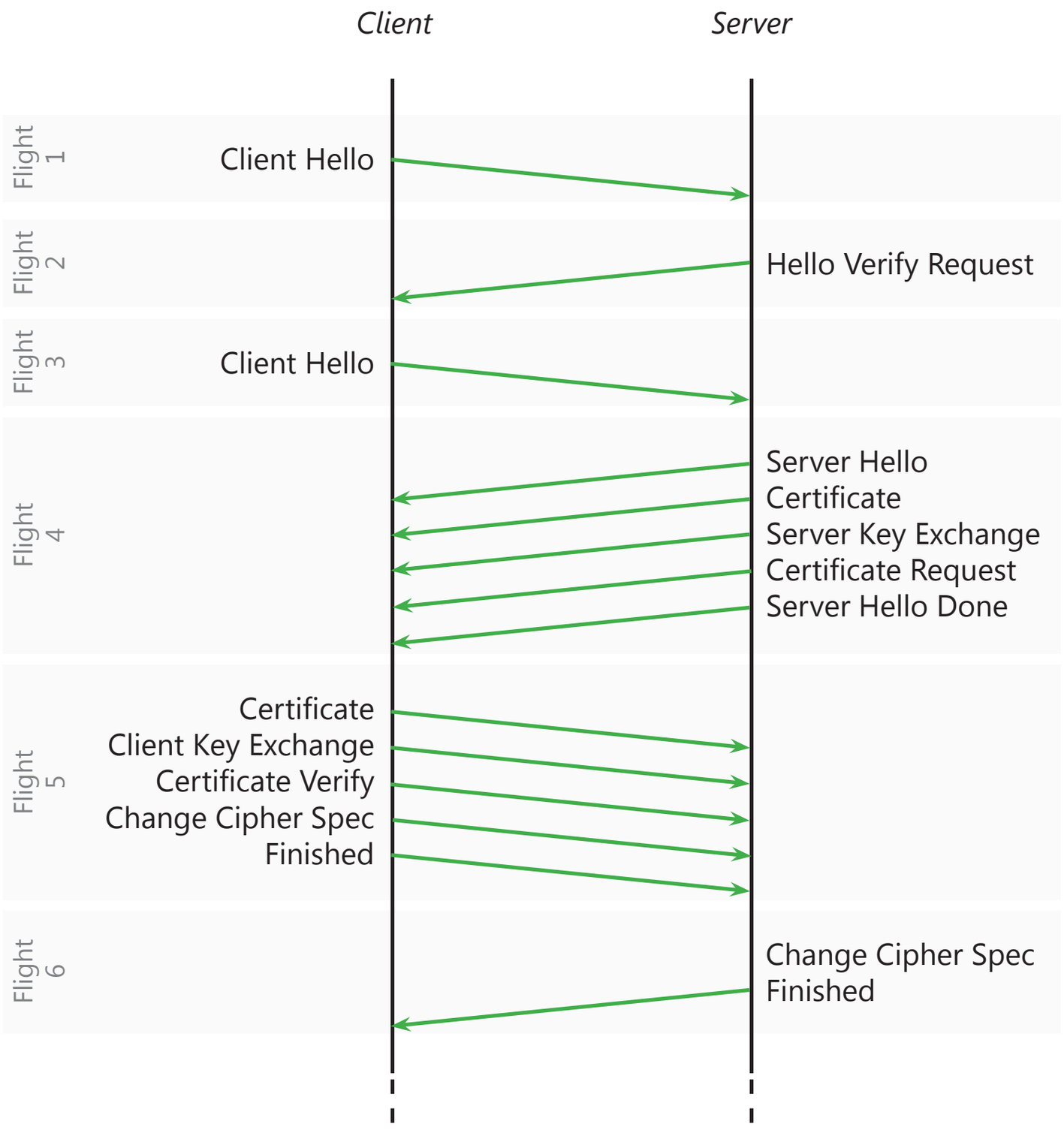
CoAP with DTLS





4 roundtrips

CoAP with DTLS



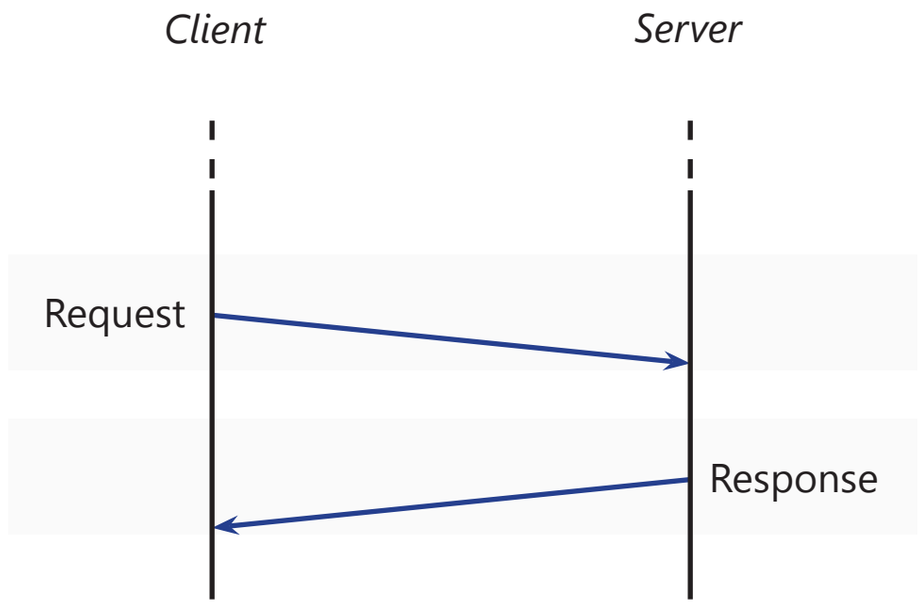
DTLS handshake over 6LoWPAN — ~ 40-50 bytes handshake message size

Raw Public Key SubjectPublicKeyInfo sizes

ECDSA_P256 — 91 bytes

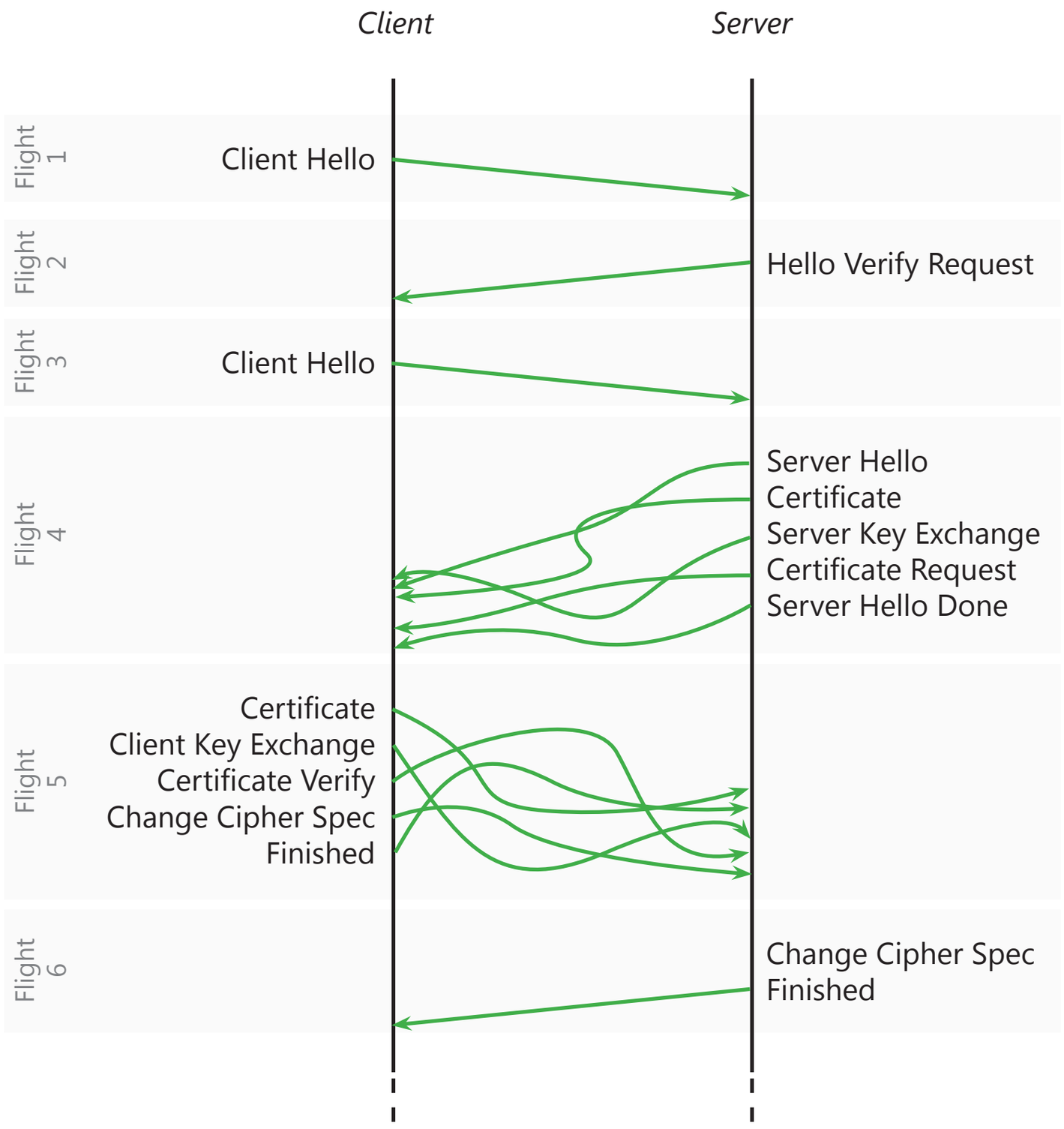
ECDSA_P384 — 120 bytes

ECDSA_P521 — 156 bytes



4 roundtrips

CoAP with DTLS



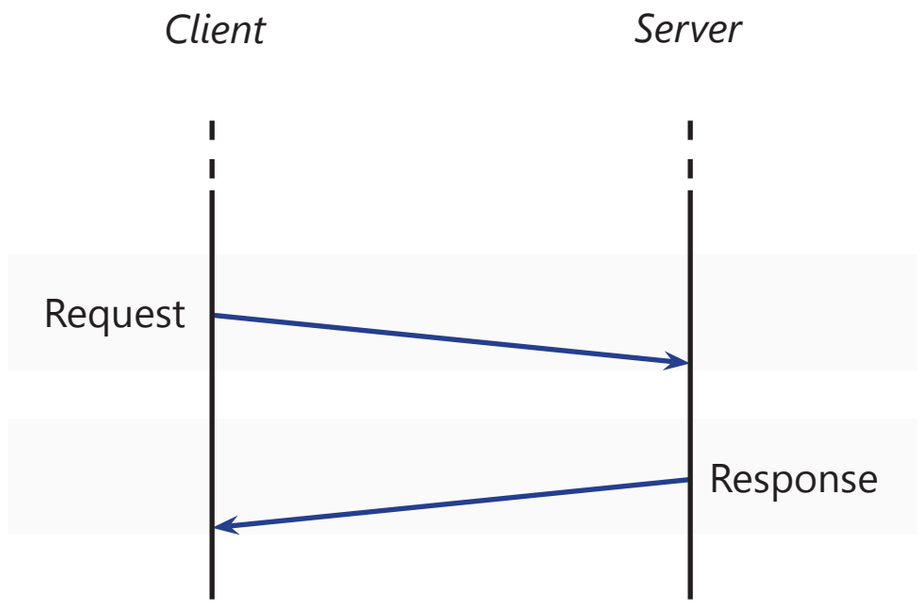
DTLS handshake over 6LoWPAN — ~ 40-50 bytes handshake message size

Raw Public Key SubjectPublicKeyInfo sizes

ECDSA_P256 — 91 bytes

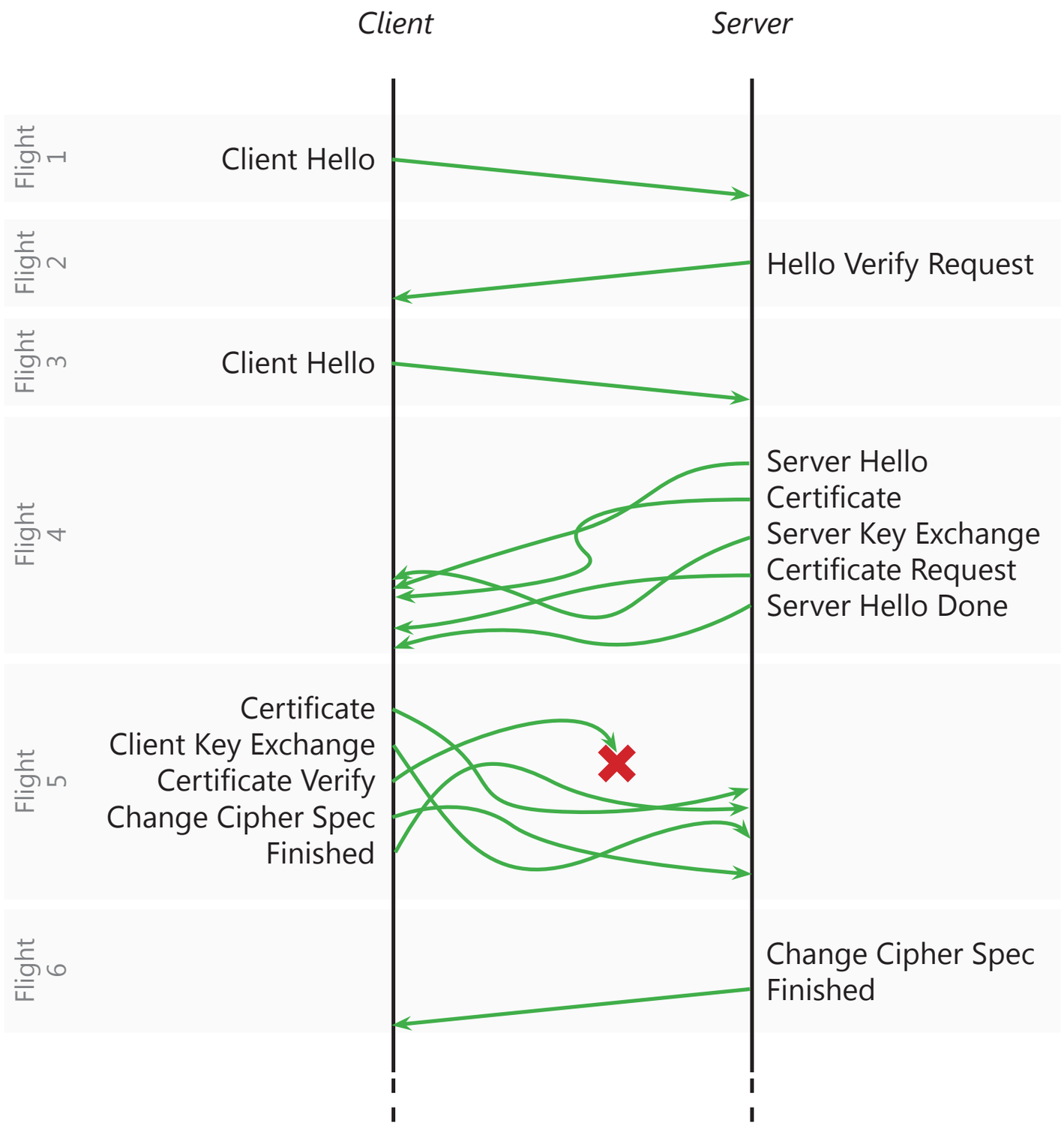
ECDSA_P384 — 120 bytes

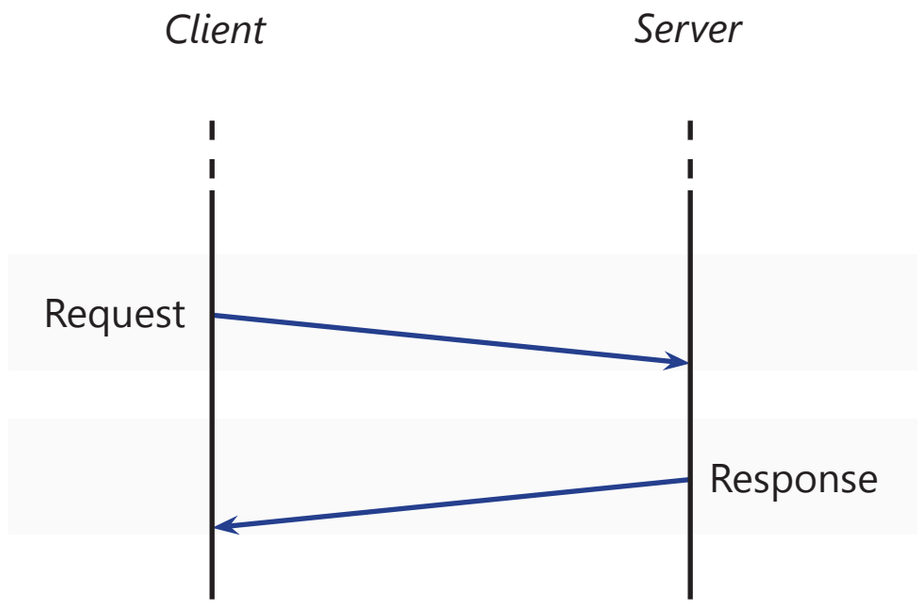
ECDSA_P521 — 156 bytes



4 roundtrips

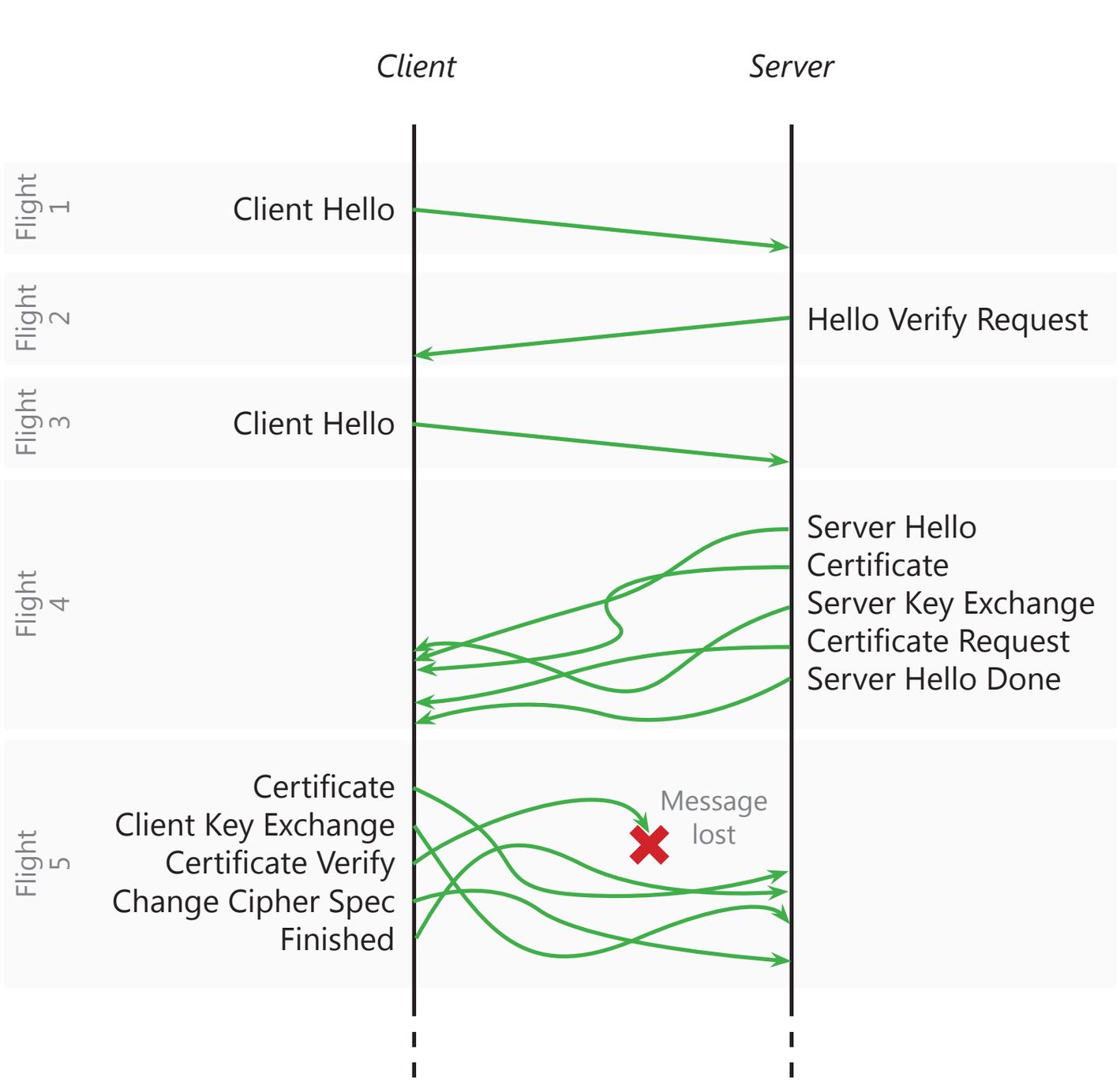
CoAP with DTLS

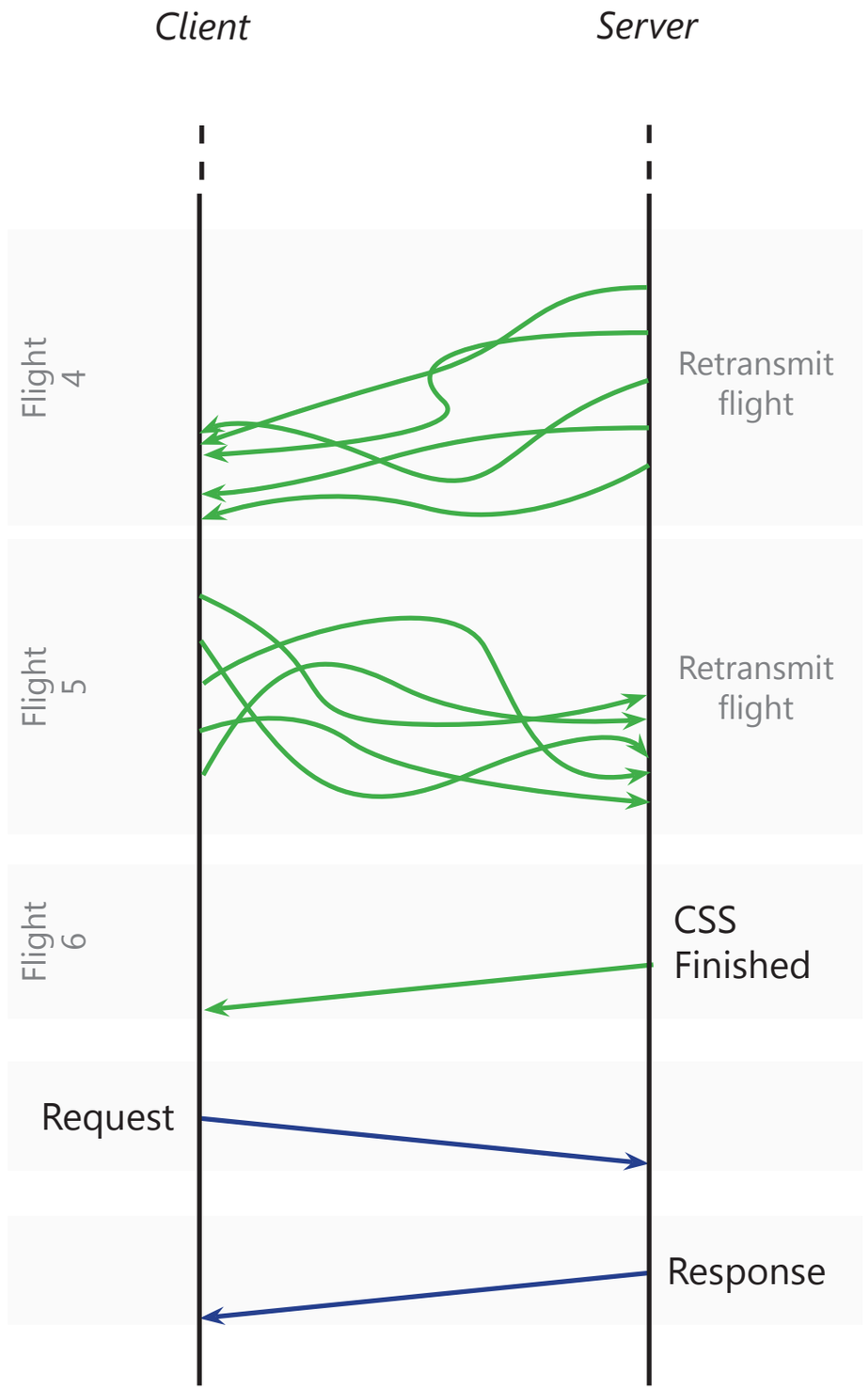




4 roundtrips

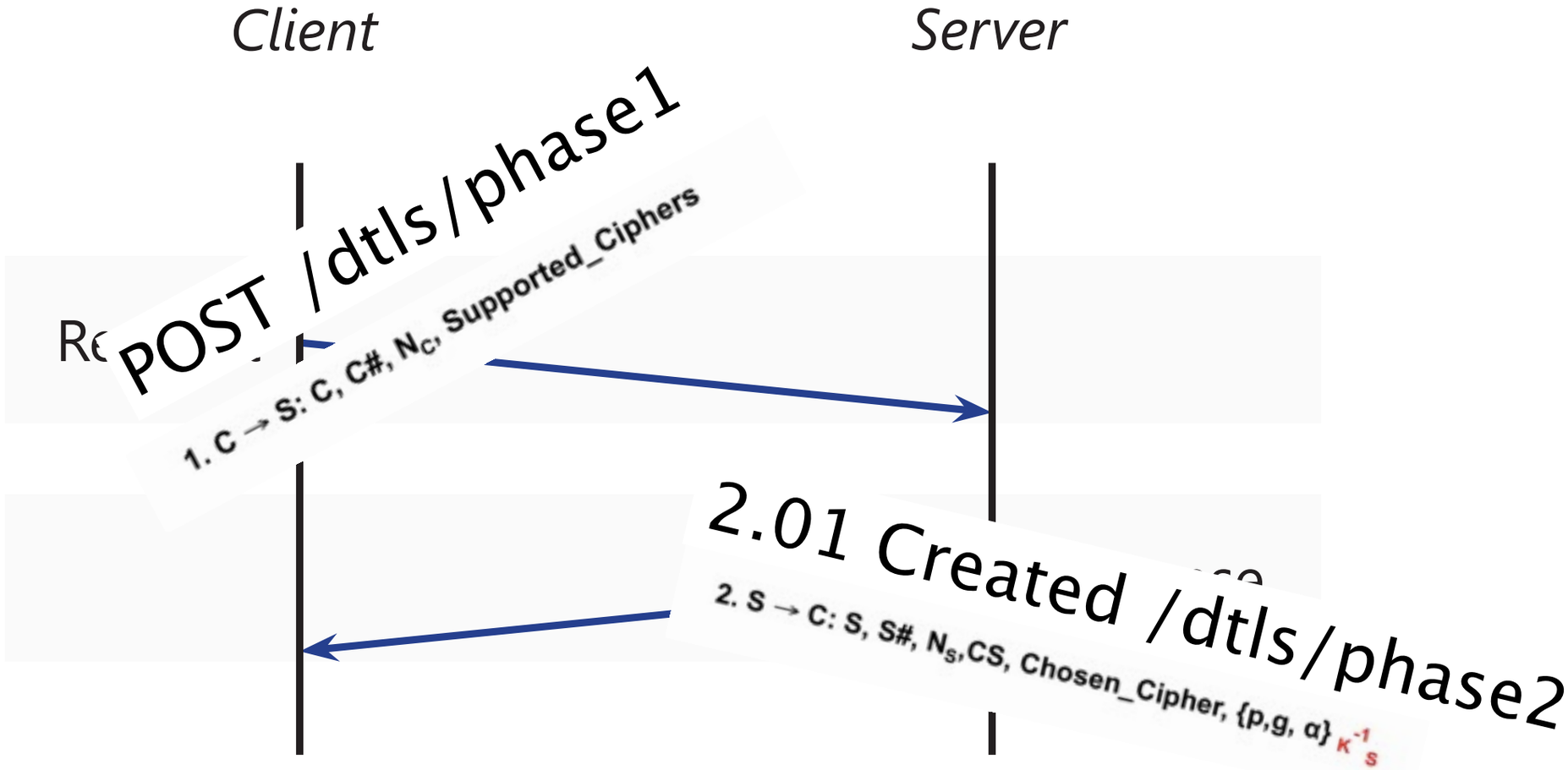
CoAP with DTLS





6 roundtrips

Using CoAP to transport DTLS?



1 roundtrip

CoAP-Block solves the large-object retransmission problem

Code Size	Description
1429 Bytes	SHA-256
992 Bytes	CCM
9812 Bytes	DTLS state machine

TABLE I
CODE FOOTPRINT OF MINIMAL DTLS IMPLEMENTATION