certificate Enrollment over Secure Transport (EST)

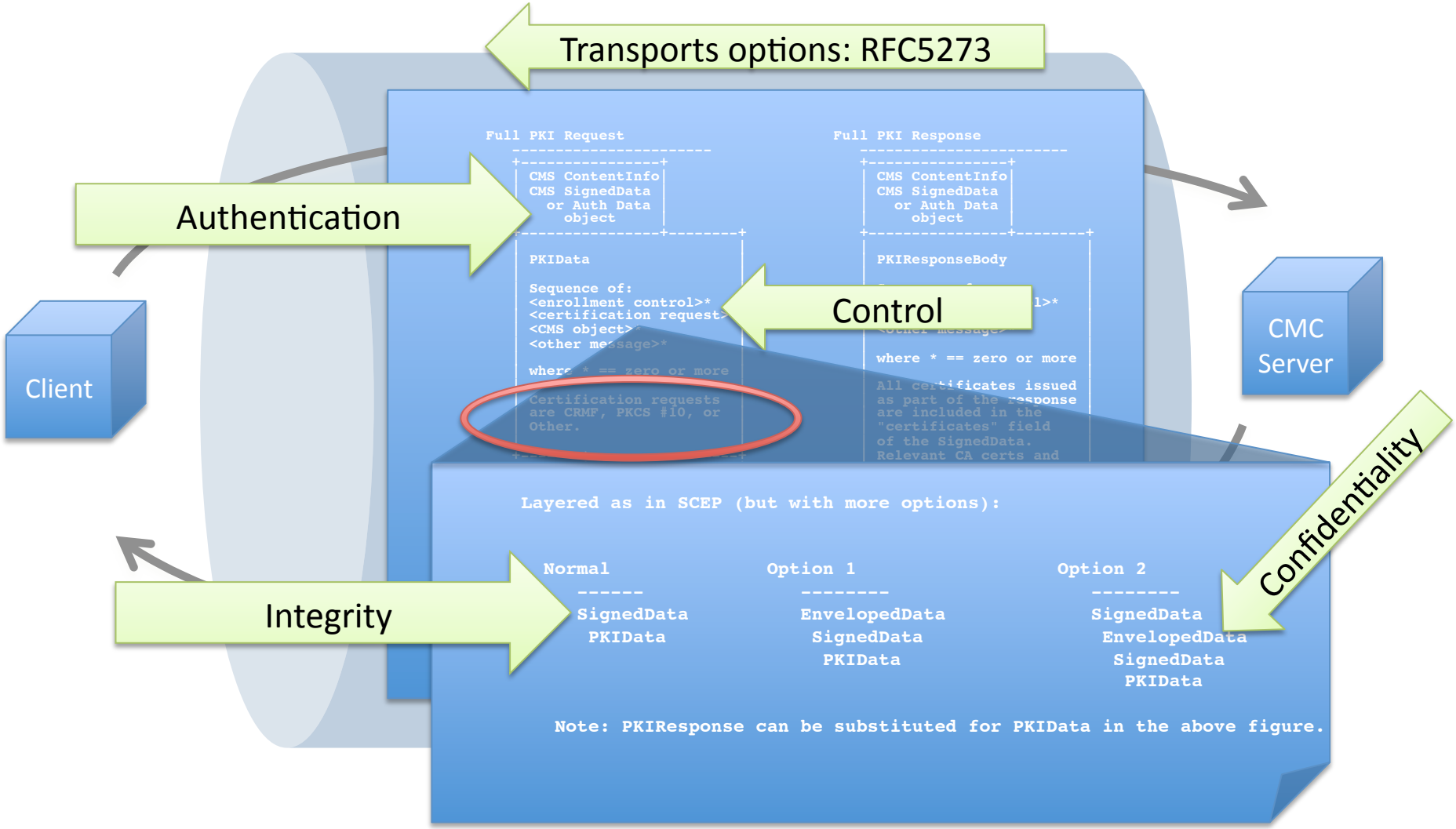
A simple and direct enrollment profile
draft-pritikin-est-00

Max Pritikin (pritikin@cisco.com)
Joseph Salowey (jsalowey@cisco.com)

Certificate Enrollment going forward

- Goal is to enable certificate enrollment to get certificates on to as many types of devices as possible
  - Simplify Enrollment Process

CMC review (simplified)



Message Oriented Issues

- Existing Enrollment Protocols focus on providing security services independent of transport
  - Leads to security mechanism that are only used in enrollment protocols
  - Lack of integration with other systems
  - Implementation is more difficult

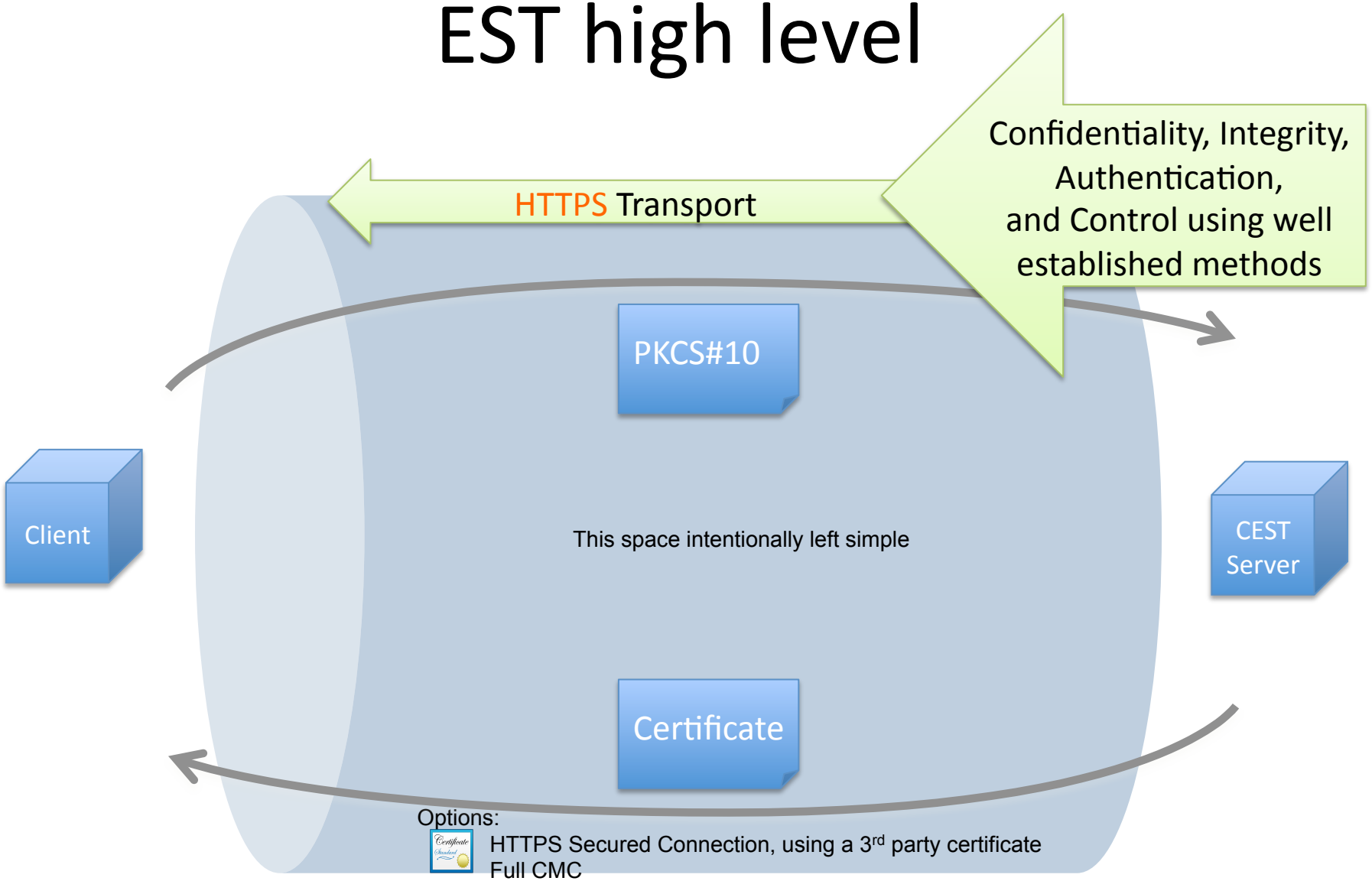
EST Motivation

- Simplify implementation by leveraging Secure Transport
  especially for clients, but also for servers
- Profile of CMC and SCEP overlap
  - 'CMC: Transport Protocols' compliant
  - Path forward for SCEP implementations
  - CMC profile
- Re-key/re-enroll from CMP
- ECC Algorithm Support
  - Suite B compatibility

  … and keep it simple

  Oh, with an obvious growth path that parallels the current industry

EST high level



Simplifying

Drop transport independence in favor of:

TLS for authentication and confidentiality

HTTP headers for status

- HTTPS is common and simple. Well proven. Widely Implemented and Deployed
- Lots of authentication and authorization options
  - Certificates during TLS
  - HTTP methods
  - Room to grow

Conclusion

- Proposal
  draft-pritikin-est-00
  Feedback actively solicited

- Sample client implementation of EST enrollment:*

```
curl $URL -s -d $PKCS10FILE -o $NEWCERT –E
  $EXISTINGCERT –cacert $CACERT
```

- Combines features of SCEP, CMC and CMP
  (re-enroll uses CMP defined method, see draft for details)
  A ‘way forward’ at for PKIX enrollment protocols meeting the needs of simple clients and clarifying some of the confusion

*Command line options may vary

Questions

?

EST high level
(Leverage Secure Transport)