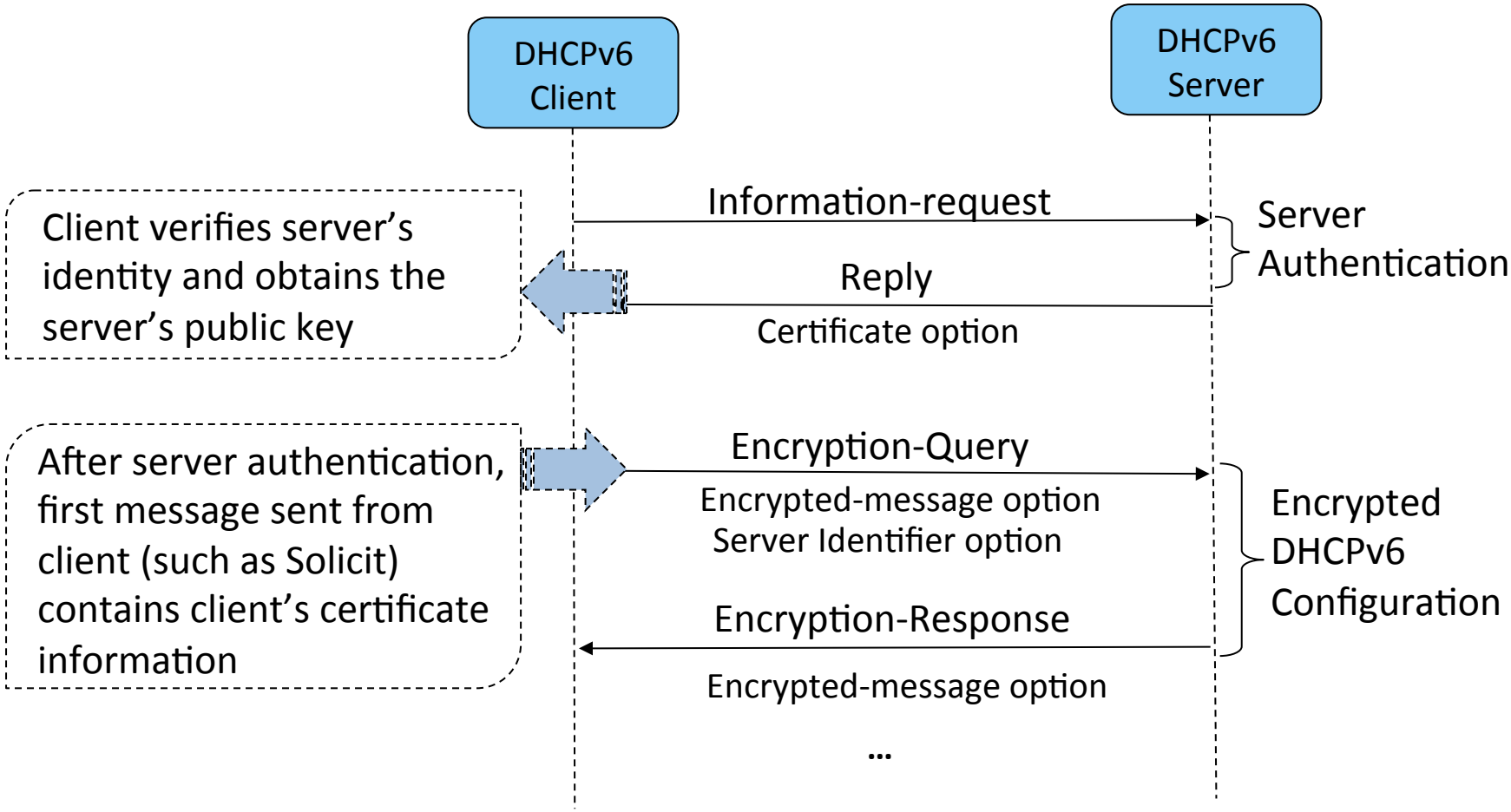
Secure DHCPv6

draft-ietf-dhc-sedhcpv6-11

Presenter: Ted Lemon

Secure DHCPv6 Overview



Update after IETF94

- Remove the Signature option
  - For the Reply message, only content is Certificate option. The client is already expected to validate it directly (by comparing it with locally pre-configured info). So we do not necessarily need to provide additional integrity protection
  - The subsequent encrypted messages also don't need the signature option for integrity check

Update after IETF94

- Reserve the timestamp option
  - Provide anti-reply protection for encrypted messages
- Add the encryption algorithm negotiation process;
  - The certificate option adds the EA-id (encryption algorithm identifier) field

Update after IETF94

- Rewrite the "Applicability" section
  - Deployment scenario
    - Clients and servers are pre-configured with trusted certificates info
    - Example scenario: enterprise network
  - Add explanation of advantage of secure DHCPv6 against security mechanism in RFC3315
  - More widely applicable with integration of generic PKI is subject to future study and out of scope

Update after IETF94

- Modify client behavior when there is no authenticated DHCPv6 server
  - The client should retry a number of times to beat out a busy “real” server
  - And then take some alternative action depending on its local policy, such as attempting to use an unsecured DHCPv6 server

Update after IETF94

- Add the DecryptionFail error code
  - If the message from client fails decryption, the server sends Reply message with DecryptionFail error code
  - Upon receiving a DecryptionFail error status code, the client MAY resend the message following normal retransmission routines defined in RFC3315

Open Issues

- Remove of public key
  - Reason
    - Self-signed certificate can replace public key if the device is pre-configured with public key, not certificate
    - According to locally pre-configured info, self-signed certificate can be verified
  - Disadvantage
    - Size of message is increased when public key is actually needed, not certificate

Open Issues

- Secure DHCPv6 changes DHCPv6 message exchanges
  - Caused changes
    - Server selection is done at key exchange phase (initial Information-request and Reply exchange)
    - Solicit can be sent only to a single server
  - Two choices
    - Make the server selection behavior more compatible
    - Accept we give up the previous server selection feature for privacy

Next Step

- Next Step?
- Thanks!