Authentication and Encryption Mechanism for DHCPv6

draft-cui-dhc-dhcpv6-encryption-01

Yong Cui, Lishan Li, Jianping Wu,Lee Yiu

Presenter: Tianxiang Li

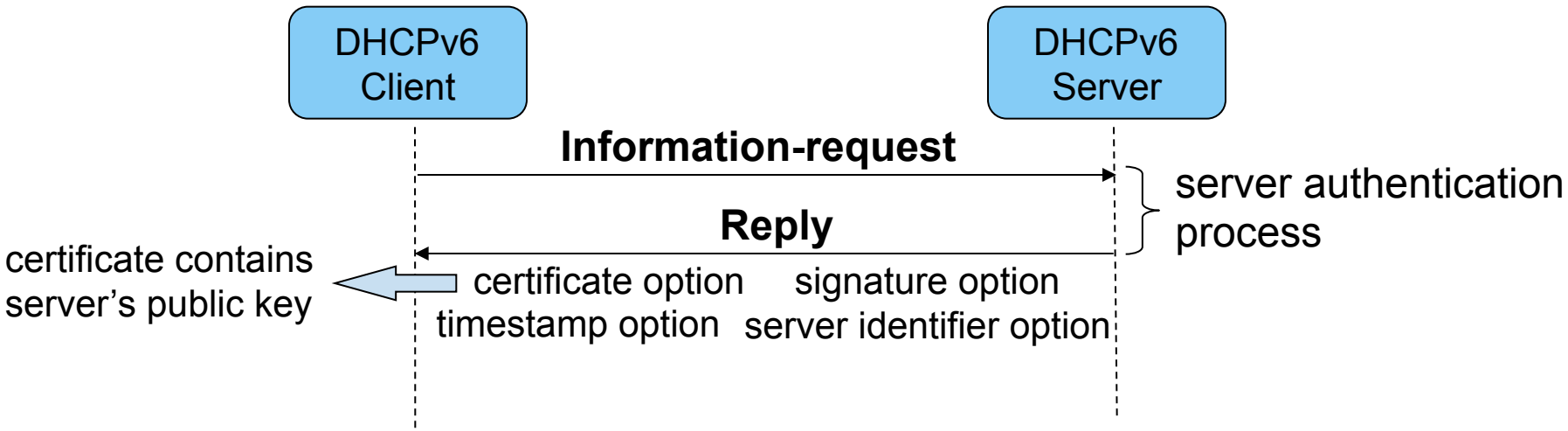
Motivation

- DHCPv6 privacy vulnerabilities
  - Various identifiers (draft-ietf-dhc-dhcpv6-privacy-00)
  - Many attacks, particular pervasive monitoring (RFC7258)
- Current DHCPv6 protection mechanisms
  - Secure DHCPv6
    - Do not protect message content
    - vulnerable to pervasive monitoring
  - Anonymity Profile
    - Limit the use of certain options
    - Difficult to protect newly defined options
- This document proposes **server authentication** and **encryption** between DHCPv6 client and server

Design principles

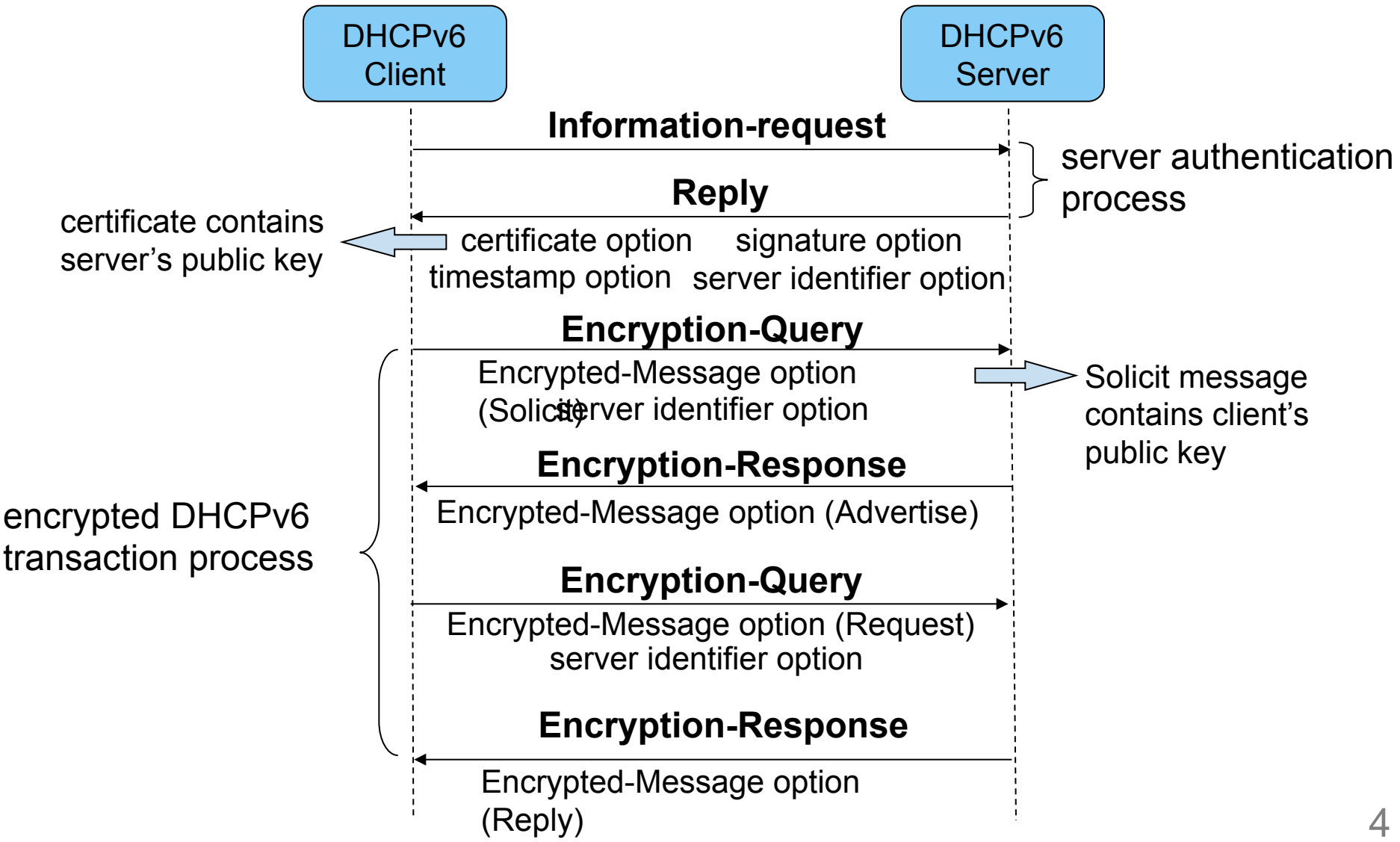
- Goal
  - Verify server's identity
  - Protect all the identifiers in the DHCPv6 message
  - Prevent pervasive monitoring
- Two-step process:
  - Server authentication
  - Encrypt DHCPv6 transaction using public keys

Solution Overview



- Server authentication
  - **Using Information-request to get server information**
    - Client multicasts Information-request message to servers, asking for the related authentication options
    - Server sends Reply message containing server's certificate, signature, timestamp, and DUID
    - If verification successful, client stores server's public key and DUID

Solution Overview

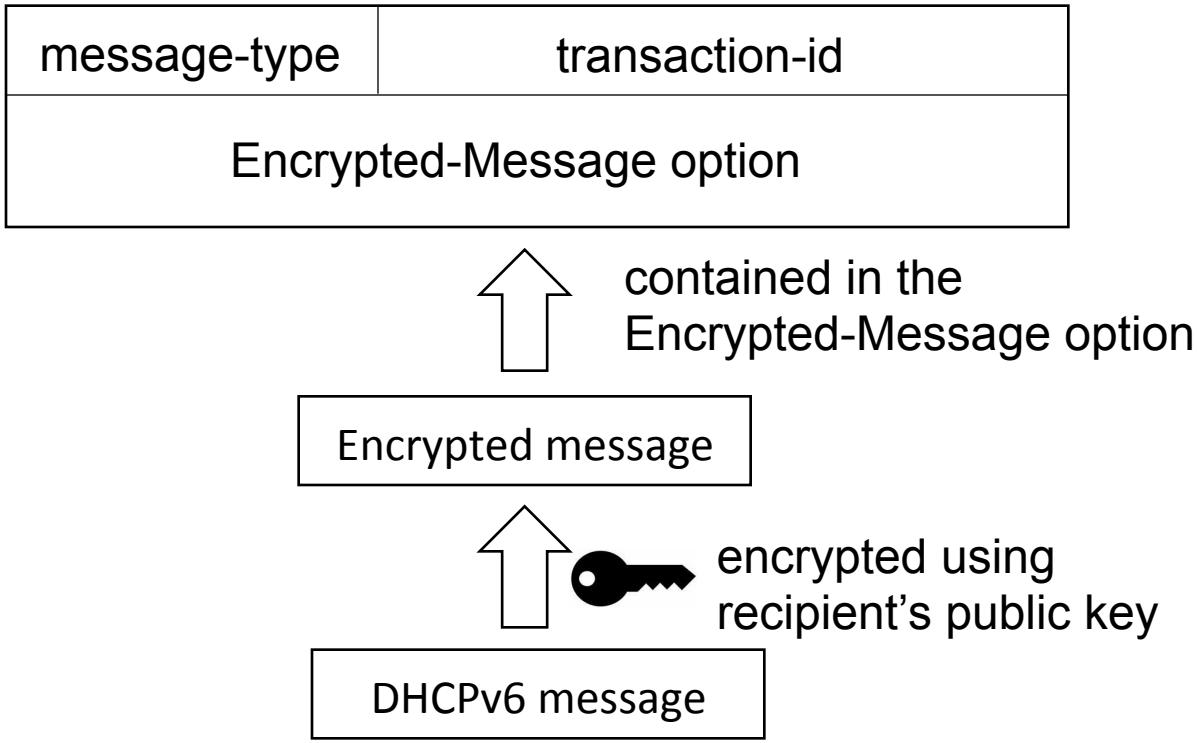


Encrypted DHCPv6 transaction

- **One new option:** Encrypted-Message option
  - Contains encrypted DHCPv6 message
- **Two new messages**:
  - Encryption-Query
    - Contains the encrypted DHCPv6 message sent by client
    - Contains the server's identifier option, to avoid untargeted servers from decrypting the DHCPv6 message
  - Encryption-Response
    - Contains the encrypted DHCPv6 message sent by server

Encrypted Message Format

- Encrypted-Query/Encrypted-Response message

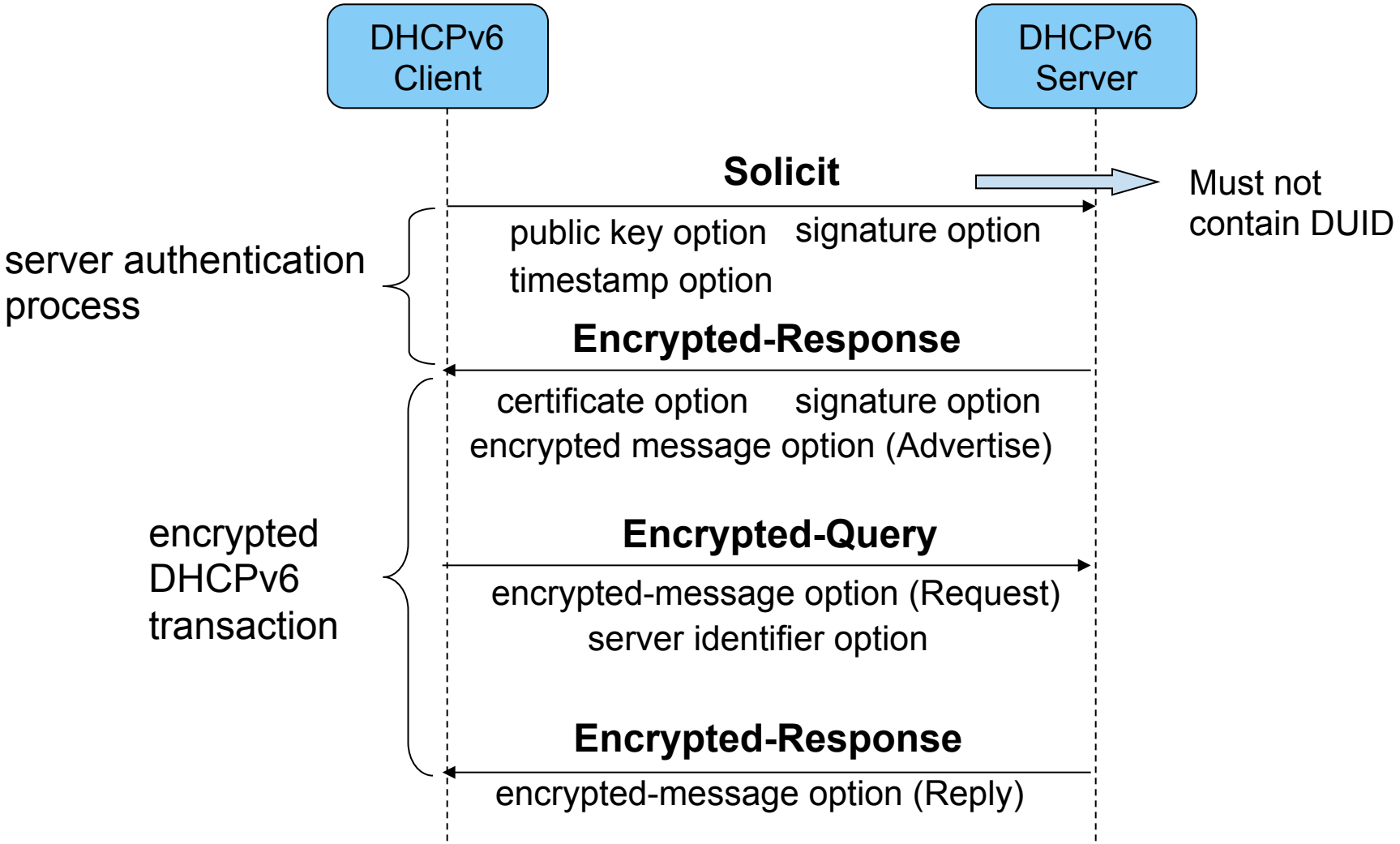


Next Steps

- Comments and reviews appreciated
- Move forward in WG?
- Thank you

Appendix: Solution B

- Authentication with Encrypted DHCPv6



Comparison

Solution A	Solution B
No change to RFC3315	Solicit message MUST NOT contain the DUID option
Need to send Information-request before DHCPv6 transaction	No change to the DHCPv6 transaction process
Select one DHCPv6 server before the DHCPv6 transaction	No change to the current server selection
Newly defined DHCPv6 messages and options Encrypted-Query/Encrypted-Response/Encrypted-Message option	