LIS Discovery

draft-ietf-geopriv-lis-discovery – Martin Thomson

Authentication

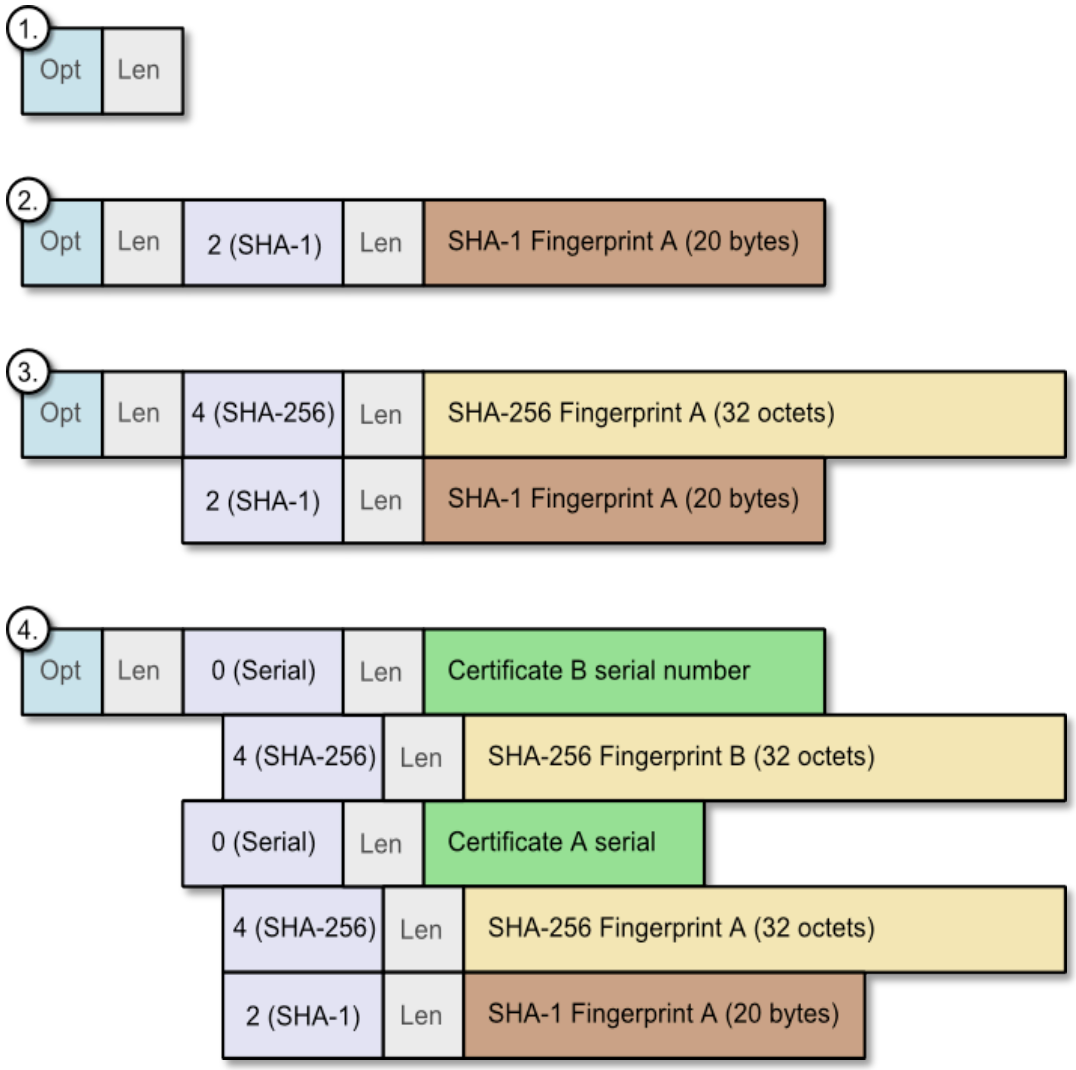
- One major change since -04 (last meeting)
  - Option to authenticate the LIS using certificate fingerprints was added in -05
- DHC review of -05
  - Option format in -07 is based on the DHC review
- secdir review revealed operational issues with initial design. Authentication would reject:
  - Certificates as they expired and were replaced
  - Alternative hosts with different (but valid) certificates
  - Addressed in -08…as I will explain

LIS certificate fingerprints

- Authentication uses LIS certificate fingerprint option
- Uses sub-options format from -07:
  - The sub-option code identifies the hash function used to generate the fingerprint
    - Copies code points from the TLS HashAlgorithm registry
  - **In -08**: Sub-option 0 includes a certificate serial number
    - Fingerprint sub-options following this sub-option only apply to the certificate with that serial number

Authentication Algorithm

- If the LIS certificate fingerprints option is empty:
  - Use domain name-based authentication: RFC2818
- If the option contains any data:
  - The LIS is unauthenticated unless a fingerprint matches
  - Match the first fingerprint with a supported hash algorithm
  - **In -08**: Certificates may be identified by a serial number
    - Only check fingerprints where the serial number matches
    - Avoids problems with certificate expiry, alternative certificates
    - No serial number required if there is only one certificate



Structure and Usage Examples

1. No fingerprint: use domain name
2. Simple option: single fingerprint
3. Upgrade hash algorithm: place preferred hash first
4. Replace certificate: identify certificates using serial numbers

Next steps

- Need to finalize option format with DHC
- No other open issues on document
- **WGLC once format is finalized?**