Secure DNS RR Update for ACME DNS Based Challenges

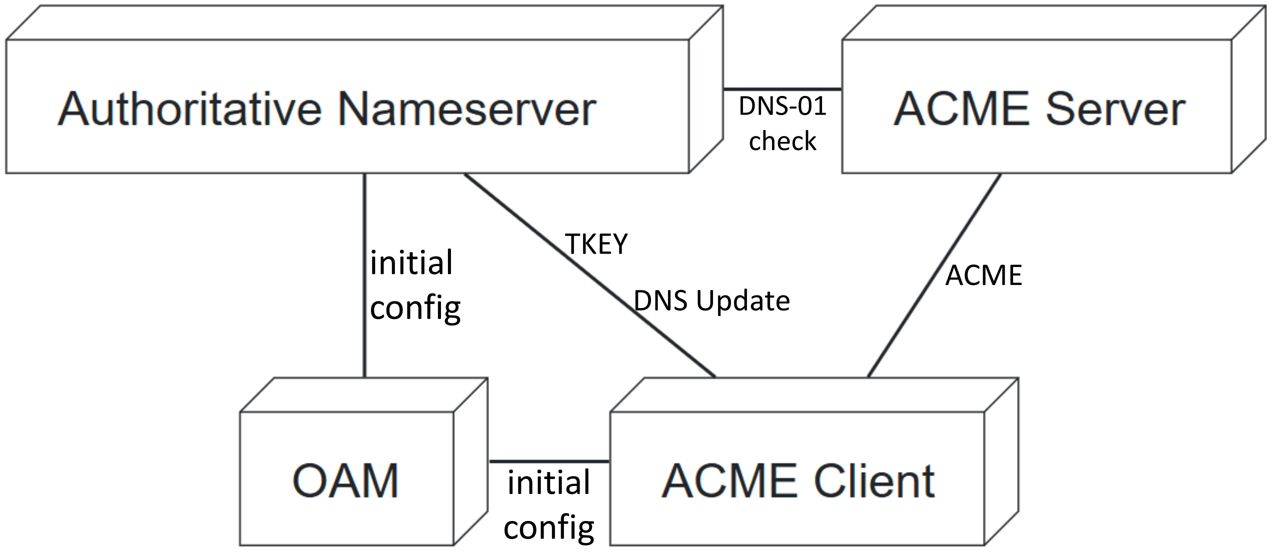
draft-li-acme-dns-update

Ruochen Li, Haiguang Wang, Zhongding Lei

Problem Statement

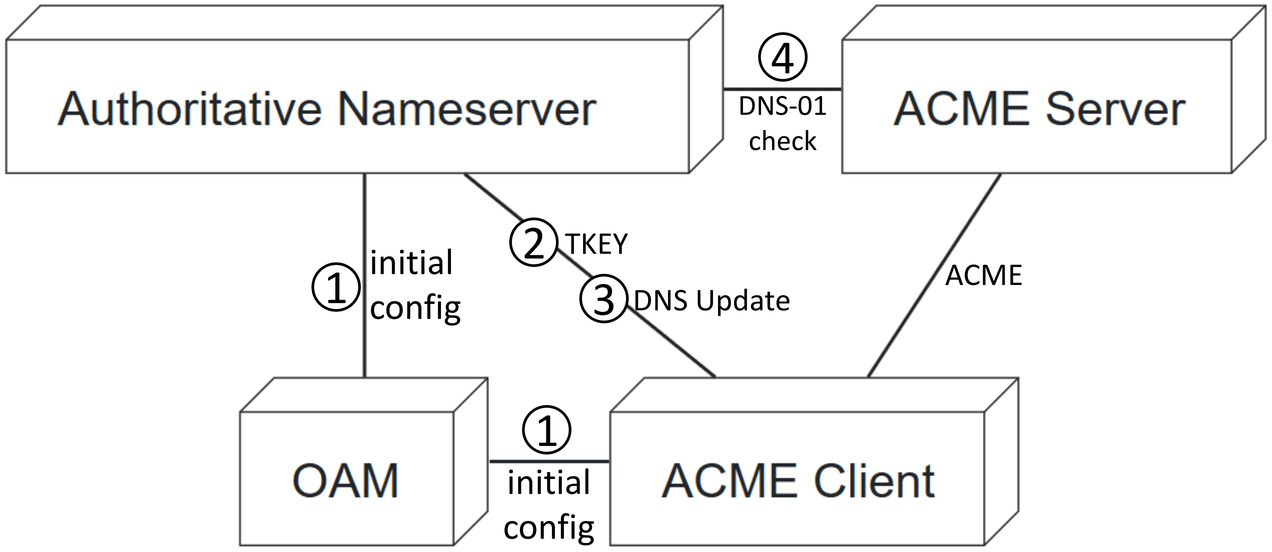
- **ACME DNS Challenges**: Require clients to prove domain control via DNS records (e.g., TXT entries).
- **Gap**: No recommended procedure for secure DNS record updates for ACME.
- **Solution**: Define a recommended DNS challenge procedure using ***DNS UPDATE*** (RFC 2136) with ***TSIG*** (RFC 8945) and/or ***SIG(0)*** (RFC 2931) for authentication.

Architecture Overview



- **OAM** configures initial TSIG keys for clients.
- **ACME Client** uses keys to authenticate DNS updates.
- **Authoritative Nameserver** validates updates via access control.
- **ACME Server** verifies records for certificate issuance.

Procedure Overview



1. Initial Setup
    - OAM configures domain and TSIG/SIG(0) keys on client & nameserver.
2. (Transaction Key)
    - Client establishes transaction TSIG key (via TKEY RFC 2930).
3. DNS Update
    - Client adds/removes ACME DCV records (TXT) with TSIG.
4. DNS Challenge Validation
    - ACME server fetches records to confirm domain control.

Initial key:	**Txn key:**
TSIG	TSIG
SIG(0)	SIG(0)

Things to Consider

- Access control of the keys on the DNS server (for DNS Update and transaction key establishment, restrict to specific domains/record types)
- DNS Update replay prevention
- Key rotation, short-lived keys
- Apply DoT/DoH to encrypt DNS Update traffic
- Clean up after use (DCV records & transaction keys)

Thank You!