Important Notes of Using Domain Name Ownership / Control Verification by DNS

▼Scope of this memo

Some services on the Internet verify **ownership / control of subscribers' domain name** by using DNS name resolution. This memo describes **the mechanisms of the verification and recommended actions by related parties**.

▼Use cases

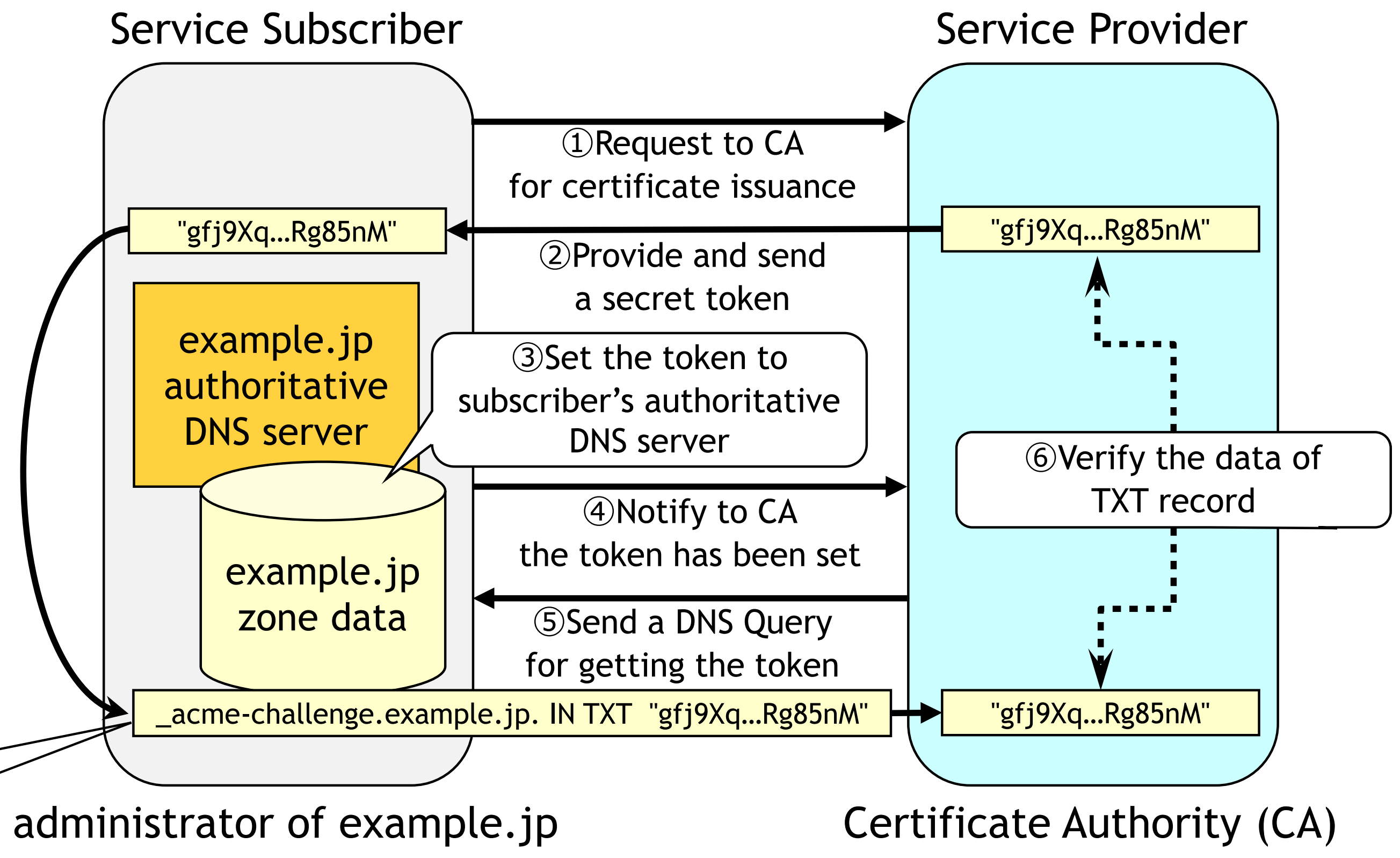
- Issuance of server certificates (**dns-01** on ACME, see below)
- Providing web CDN services
- Providing groupware services on subscribers' domain names

▼Mechanisms of the verification

The **"challenge-response" mechanism** is commonly used for DNS-based ownership / control verification.

In the beginning, the service provider makes **a one-time secret token** and sends to the service subscriber in a secure manner. And the service subscriber sets the token on **its authoritative DNS server in a certain way**.

Then the service provider gets the data set by the service subscriber using **DNS name resolution**, and **verifies the DNS data**.


Service Subscriber
Service Provider
①Request to CA for certificate issuance
"gfj9Xq...Rg85nM"
②Provide and send a secret token
"gfj9Xq...Rg85nM"
example.jp authoritative DNS server
③Set the token to subscriber's authoritative DNS server
⑥Verify the data of TXT record
④Notify to CA the token has been set
example.jp zone data
⑤Send a DNS Query for getting the token
_acme-challenge.example.jp. IN TXT "gfj9Xq...Rg85nM"
"gfj9Xq...Rg85nM"
administrator of example.jp
Certificate Authority (CA)

dns-01 uses underscored label "**_acme-challenge**" for verification. This label is reserved by IANA.

Figure 1: Flow of the verification by dns-01 on ACME

▼Recommended actions by related parties

- **Protocol developers**
  - **Select underscored label(s)** for protocols / services and **register to the IANA**
- **Service providers**
  - **Enable DNSSEC validation** on its full-service resolvers for verification
- **Service subscribers**
  - **Apply DNSSEC** on its authoritative DNS servers
- **External DNS service providers**
  - **Provide DNSSEC service** for its customers
  - Ensure that **underscored subzones of existing zones cannot be configured by other customers on the same authoritative DNS servers**

▼Related RFCs and standardization status

RFC 8552 and 8553 (BCP 222) defines a semantic scope for DNS record types that are associated with the parent domain name above the underscored labels, and creates the **"Underscored and Globally Scoped DNS Node Names" registry** on the IANA.

The **draft-ietf-dnsop-domain-verification-techniques** recommends to use **TXT record with underscored label per service** as **"_foo-challenge"** and **"_feature1._foo-challenge"** for multiple features. This draft is now discussed on **IETF dnsop WG** (now in WG Last Call).

Information of this memo is as of March 2023.