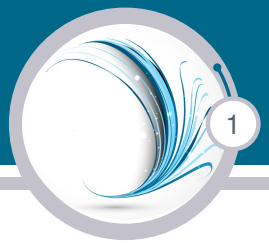
acme-conductor

Tobias Rueetschi
tr@brief.li

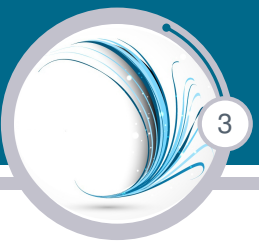
February 9, 2016

Content



Introduction
ACME

- Protocol
- Validate domain (DV certificates)
- Challenge/Response
- Used and developed by Let's Encrypt



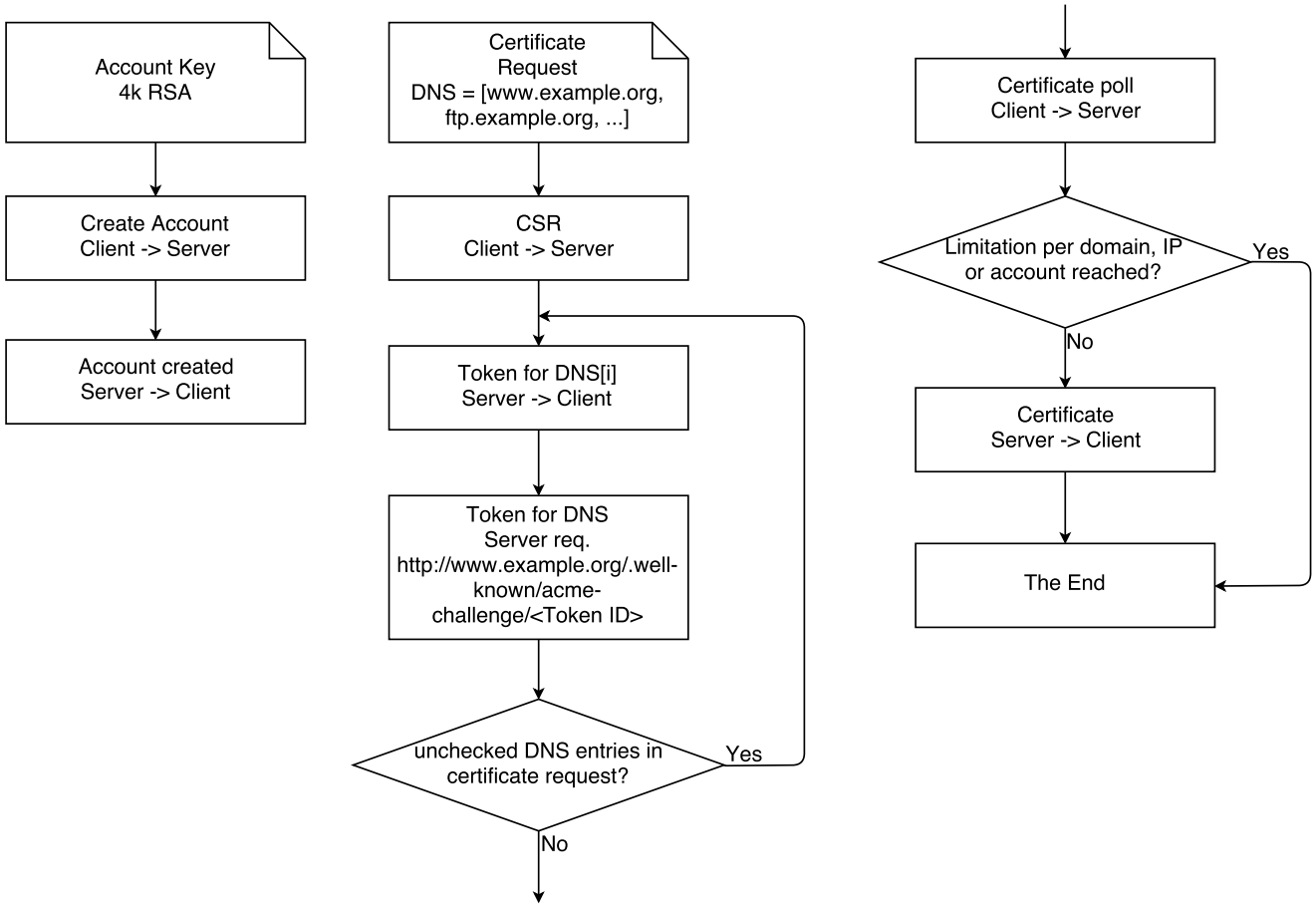
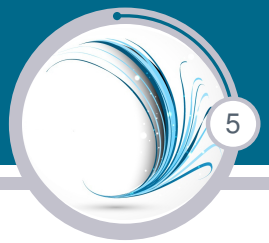


Figure: simplified ACME protocol

Introduction
Definitions

- ACME-Server: The validation server (e.g. served by let's encrypt)
- ACME-Client: The webserver from which the ACME Server get's the tokens
- Conductor: The server in the background which acts as a conductor
- ServerX, ServerY: Servers which needs the private key and certificate at the end

Introduction
Facts



- One acme-conductor instance can be used for many servers
- Written in Python
- Supports multiple ACME-Clients
- Support for split DNS
- Easy extendable

Workflow
Preusage

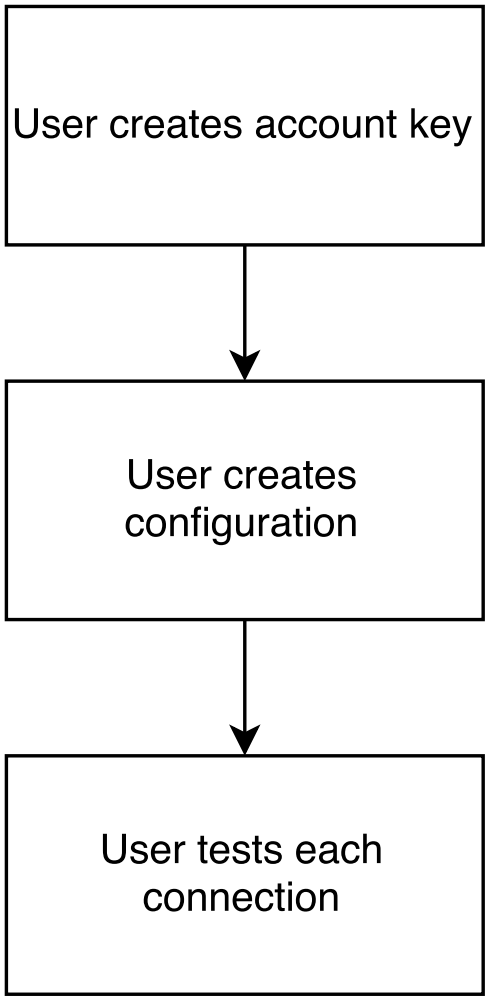


Figure: Workflow before client can be used

Workflow
Conductor

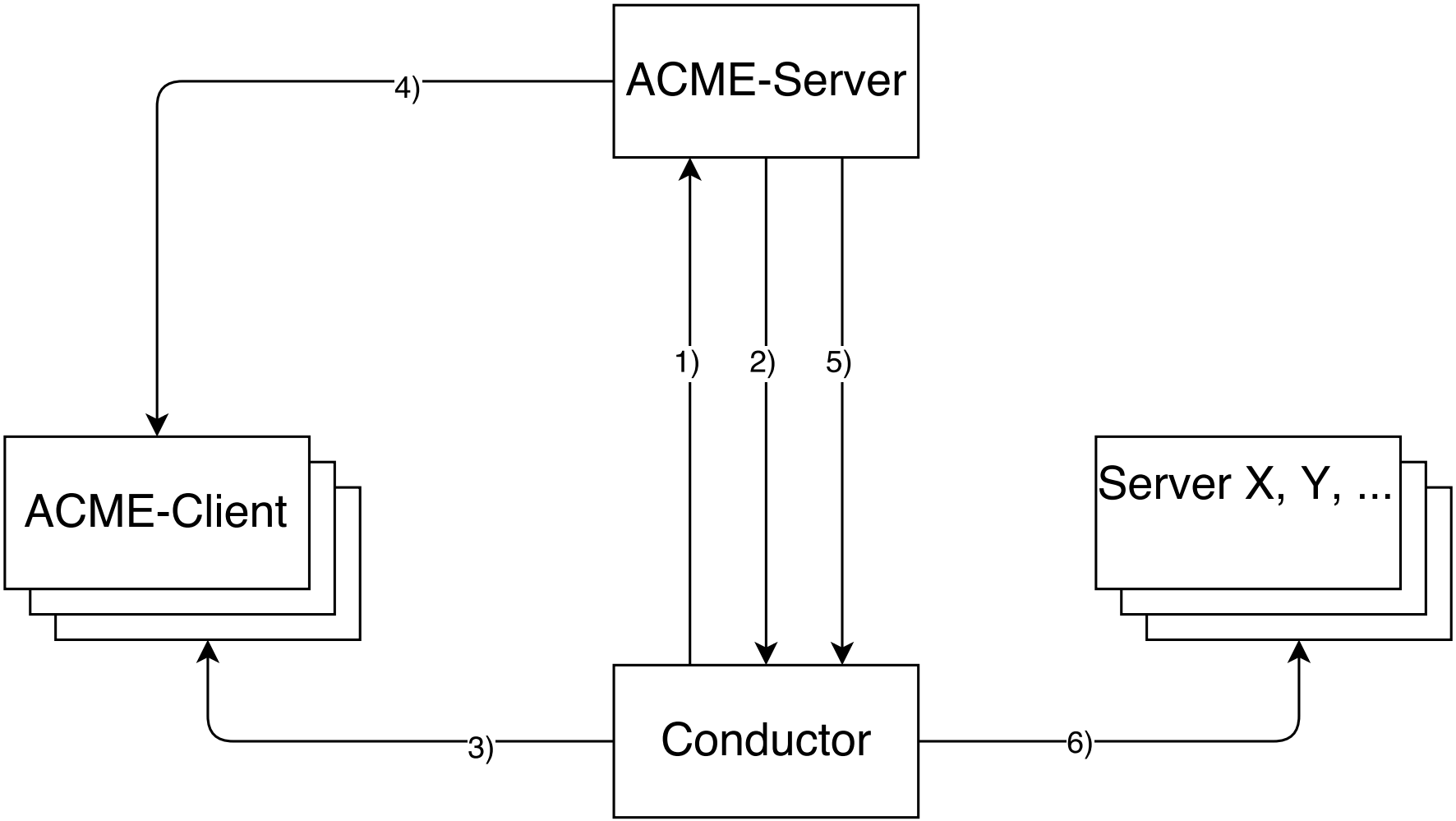
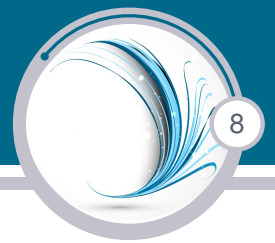


Figure: Workflow conductor

Configuration
Global values

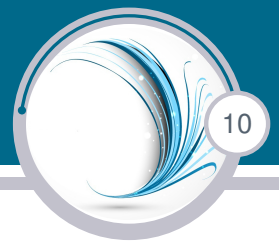



```
account_key: '/var/lib/acme-conductor/account.key'
loglevel: 'INFO'
ssl_dir: '/var/lib/acme-conductor/ssl'
keysize: 4096
file_mode: '0600'
expire: 14

#acme_server: 'https://acme-staging.api.letsencrypt.org'
acme_server: 'https://acme-v01.api.letsencrypt.org'

locality:
  country: 'CH'
  state: 'Bern'
  city: 'Bern'
  organization: 'Example'
  organizationUnit: 'Webservers'
```

Configuration
Connectors


```
ssh:
  key: '/var/lib/acme-conductor/ssh/id_rsa'
  known_hosts: '/var/lib/acme-conductor/ssh/known_hosts'
  timeout: 20
```

Configuration
Certificates

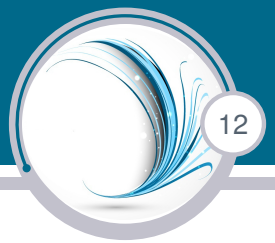



```
certificates:
  - name: 'www.example.com'
    alt:
      - 'example.com'
    acme_client: 'acme.example.com'
  - name: 'ftp.example.com'
    acme_client: 'acme.example.com'
  - name: 'mail.example.com'
    alt:
      - 'imap.example.com'
      - 'smtp.example.com'
    acme_client: 'acme.example.com'
```

Configuration
Servers

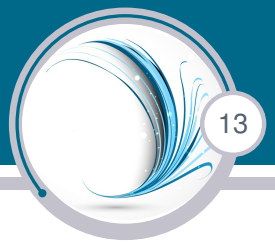

```
servers:
  - name: 'acme.example.com'
    connection: 'local'
    acme_dir: '/var/www/acme'
  - name: 'www.example.com'
    certs:
      - 'www.example.com'
      - 'ftp.example.com'
      - 'mail.example.com'
    connection: 'ssh'
    remote_dir: '/etc/ssl/local'
    command: 'service apache2 restart'
    username: 'acme'
    password: '123password'
```

Demonstration



- ACME Server: Let's Encrypt staging server
- ACME Client: A public webserver
- Conductor: local
- ServerX: The same server as the webserver
- ServerY: local

Future Work



- Support more protocols (implement more connectors)
- Support certificates without the key
- Limit server and certificates by command line options

References

[1] D. Roesler
acme-tiny
A tiny script to issue and renew TLS certs from Let's Encrypt,
https://github.com/diafygi/acme-tiny.

[2] R. Barnes J. Hoffman-Andrews J. Kasten
Automatic Certificate Management Environment (ACME)
https://github.com/ietf-wg-acme/acme/

Thank you! Questions?