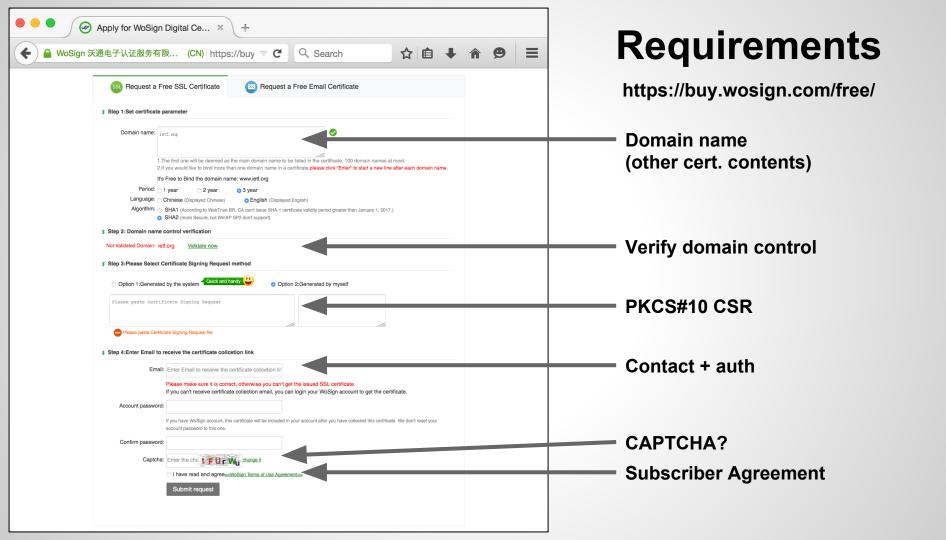
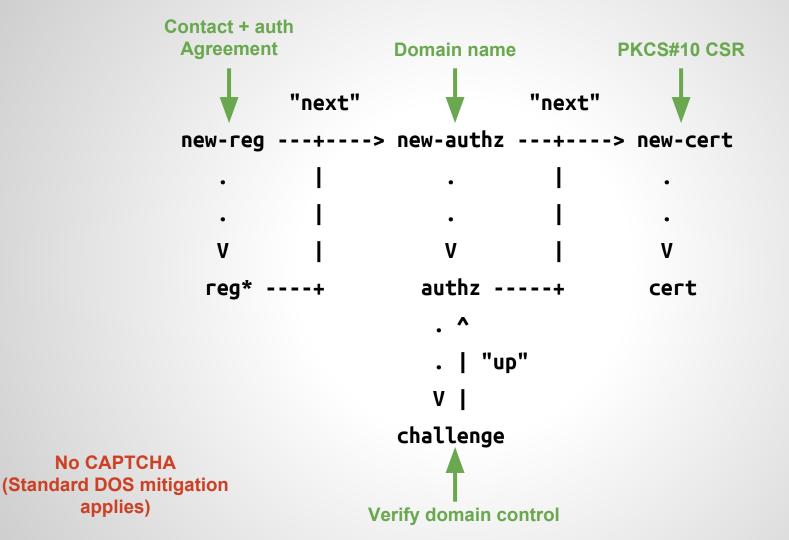


# draft-barnes-acme

# # apt-get install acme

and then...





## Registration

```
POST /acme/new-reg HTTP/1.1
                                                HTTP/1.1 201 Created
                                                Content-Type: application/json
Host: example.com
                                                Location: https://example.com/reg/asdf
  "contact": [
     "mailto:cert-admin@example.com",
                                                  "contact": /* copied */,
     "tel:+12025551212"
                                                  "agreement": /* copied */,
                                                  "key": /* JWS signature key */
  "agreement": "https://example.com/terms"
/* Signed as JWS with account key pair */
```

### **Authorization**

```
POST /acme/new-authz HTTP/1.1
Host: example.com
  "identifier": {
     "type": "domain",
     "value": "example.org"
/* Signed as JWS */
```

```
HTTP/1.1 201 Created
Content-Type: application/json
Location: https://example.com/authz/asdf
  "status": "pending",
  "identifier": {
     "type": "domain",
     "value": "example.org"
  "key": { /* JWK from JWS header */ },
  "challenges": [ /* next slide */ ],
```

## Challenges

```
/* Challenge: CA ---> Applicant */
 "type": "simpleHttps",
 "uri": "https://example.com/authz/asdf/0",
  "token": "IlirfxKKXAsHtmzK29Pj8A"
/* Response: Applicant ---> CA */
  "path": "Hf5GrX4Q7EB"
/* Signed as JWS */
```

To prove you control example.org please provision a file containing the string **IlirfxKKXAsHtmzK29Pj8A** in the directory:

https://example.org/.well-known/acme-challenge/

```
OK, I provisioned it to:
```

https://example.org/.well-known/acme-challenge/Hf5GrX4Q7EB

#### **Certificates**

```
POST /acme/new-cert HTTP/1.1
Host: example.com
Accept: application/pkix-cert

{
    "csr": "5jNudRx6Ye4H...FS6aKdZeGsyso",
    "authorizations": [
        "https://example.com/acme/authz/asdf"
    ]
}
/* Signed as JWS */
```

```
HTTP/1.1 201 Created
Content-Type: application/pkix-cert Location:
https://example.com/acme/cert/asdf
```

[DER-encoded certificate]

### Summary

```
POST new-registration — registration + agreement URL

POST registration + agreement — OK
```

```
POST new-authorization — authorization + challenges

POST challenge + response — accepted

GET authorization — authorization valid
```

POST new-certificate certificate

### Links

#### Specification:

https://tools.ietf.org/html/draft-barnes-acme-01

https://github.com/letsencrypt/acme-spec

#### Implementation:

https://github.com/letsencrypt/boulder

