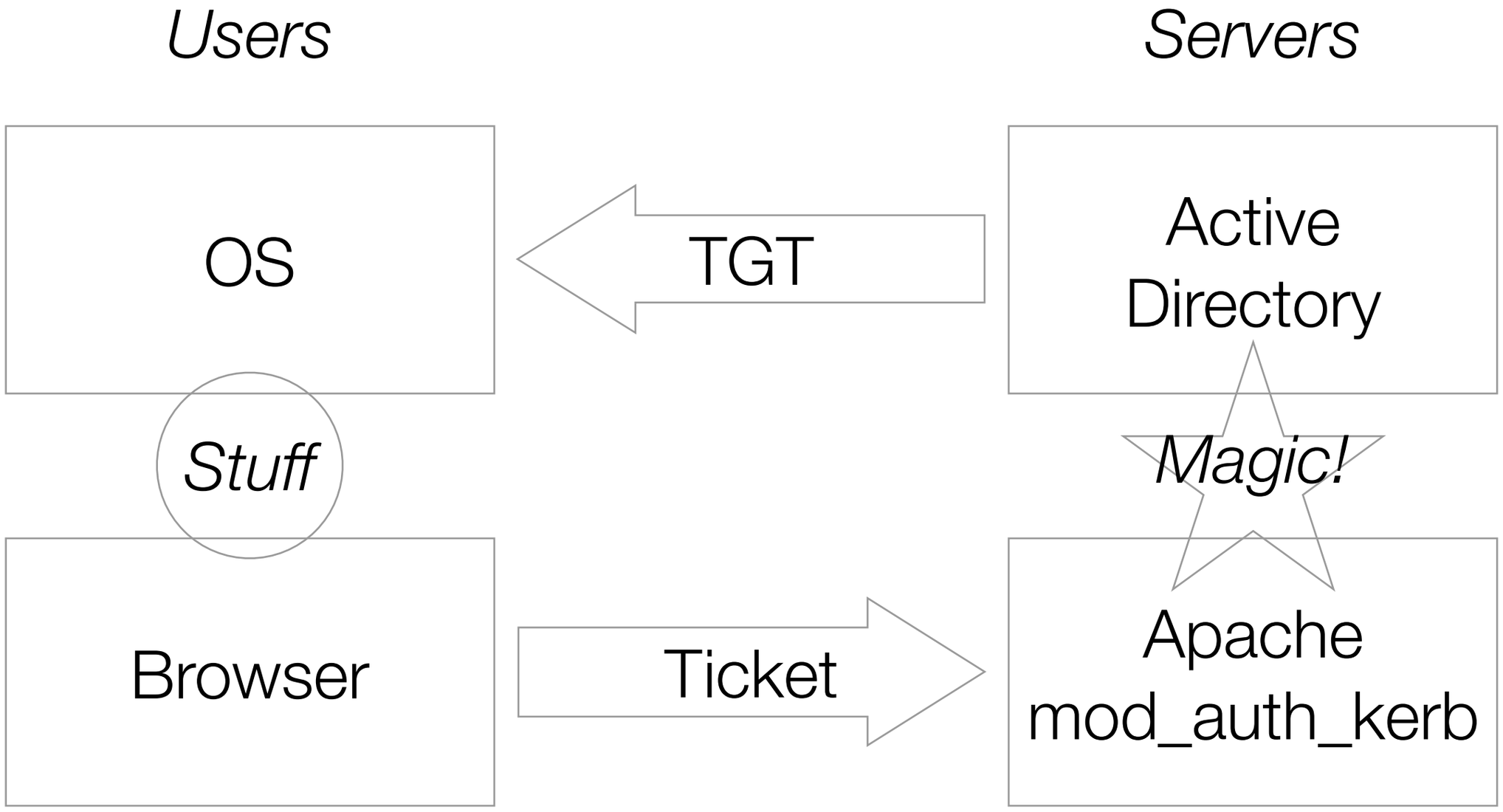
Lazy devops' guide to SSO with Kerberos

Aymeric Augustin - DjangoCon Europe - May 14th, 2014

Goal

- Provide Single Sign-On (SSO) to an internal application
  - Authentication — not authorization
- On a private network — not over the Internet

How it works


Users
Servers
OS
TGT
Active Directory
Stuff
Magic!
Browser
Ticket
Apache mod_auth_kerb

Server setup

Create a keytab

```
# msktutil --update --computer-name service                    \
           --keytab /etc/apache2/service.company.com.keytab    \
           --service HTTP

# chown root:www-data /etc/apache2/service.company.com.keytab
# chmod 640           /etc/apache2/service.company.com.keytab
```

Configure Apache

```
<Location />
   AuthName "use your corporate login to access this service"
   AuthType Kerberos

   KrbServiceName HTTP/service.company.com@COMPANY.COM
   Krb5KeyTab /etc/apache2/service.company.com.keytab

   KrbMethodK5Passwd Off
   KrbLocalUserMapping On

   Require valid-user
</Location>
```

Configure Django

```
MIDDLEWARE_CLASSES = [
    # ...
    'django.contrib.auth.middleware.AuthenticationMiddleware',
    'django.contrib.auth.middleware.RemoteUserMiddleware',
    # ...
]

AUTHENTICATION_BACKENDS = [
    'django.contrib.auth.backends.RemoteUserBackend',
]
```

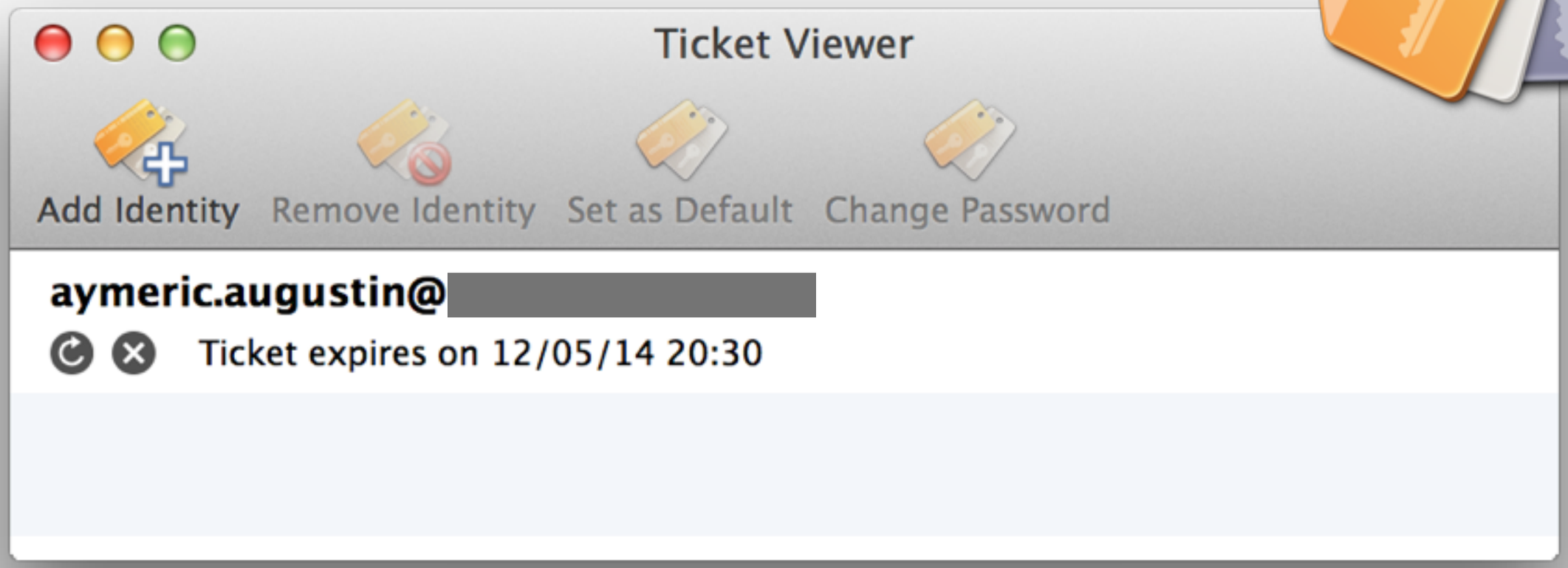
https://docs.djangoproject.com/en/stable/howto/auth-remote-user/

Client setup

Windows

- It Just Works.

OS X


Ticket Viewer
Add Identity
Remove Identity
Set as Default
Change Password
aymeric.augustin@
Ticket expires on 12/05/14 20:30

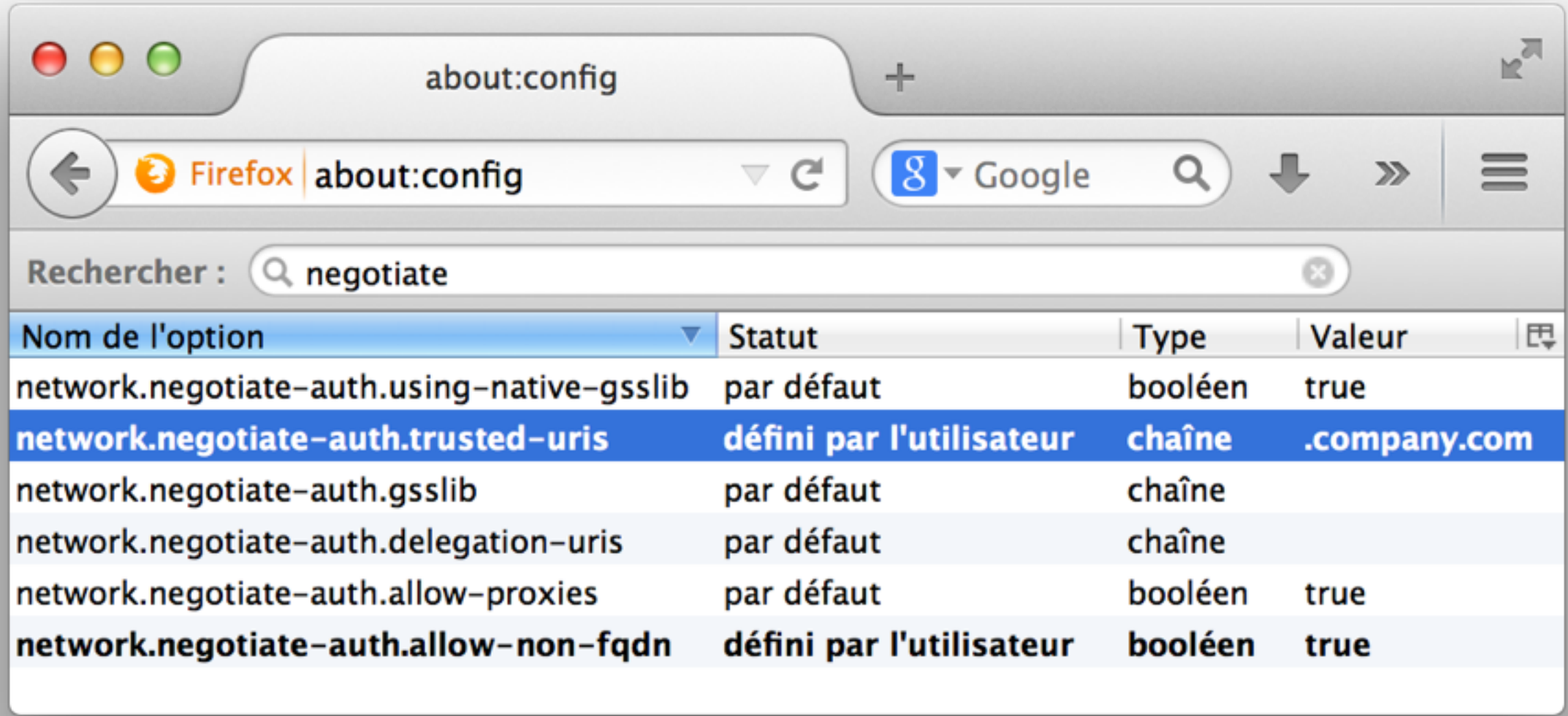
Linux or Unix

```
% kinit aymeric.augustin@COMPANY.COM
Password for aymeric.augustin@COMPANY.COM:

% klist
Ticket cache: FILE:/tmp/krb5cc_501
Default principal: aymeric.augustin@COMPANY.COM

Valid starting     Expires            Service principal
05/12/14 10:30:00  05/12/14 20:30:00  krbtgt/
COMPANY.COM@COMPANY.COM
    renew until 05/13/14 10:30:00
```

Internet Explorer

- It Just Works.

Firefox


about:config
Firefox
about:config
Google
Rechercher :
negotiate
Nom de l'option
Statut
Type
Valeur
network.negotiate-auth.using-native-gsslib
par défaut
booléen
true
network.negotiate-auth.trusted-uris
défini par l'utilisateur
chaîne
.company.com
network.negotiate-auth.gsslib
par défaut
chaîne
network.negotiate-auth.delegation-uris
par défaut
chaîne
network.negotiate-auth.allow-proxies
par défaut
booléen
true
network.negotiate-auth.allow-non-fqdn
défini par l'utilisateur
booléen
true

Chrome, Safari

- It Mostly Works.

Thank you!

https://gist.github.com/aaugustin/10715655