facebook

Issuing Certificates At Scale

Joel Goguen

Production Engineer

X.509 Certificates at Facebook

- Certificates are used for authentication
- X.509 certificates in particular

Why X.509 Certificates?

Alternatives for users?

- Passwords
  - “Hi, this is George from the Password Quality Verification Department, do you have a minute?”
- SSH keys

Why X.509 Certificates?

Alternatives for services?

- Pre-shared keys
  - “It’s time to rotate the secret. You didn’t hardcode it, right?”
- Kerberos

There is a Better Way

How To X.509

You just need a few things

- Security
- Your own CA

How to CA

```
openssl req -new -newkey rsa:4096 -keyout ca.key \
  -out ca.req –nodes

openssl ca -create_serial -out ca.crt -days 9125 \
  -keyfile ca.key -selfsign -extensions v3_ca \
  -in ca.req
```

How To X.509

You just need a few things

- Security
- Your own CA
- Trusted distribution
- Logging, logging, logging

Challenges

Number of successfully issued certificates

Every request needs a few things

- Who wants the cert?
- What do you want to do with it?
- Are you allowed to ask for this?
- How long can I give you this?
- What extra information should the certificate contain?

“Sed quis custodiet ipsos custodes?”

— Juvenal, Satire VI

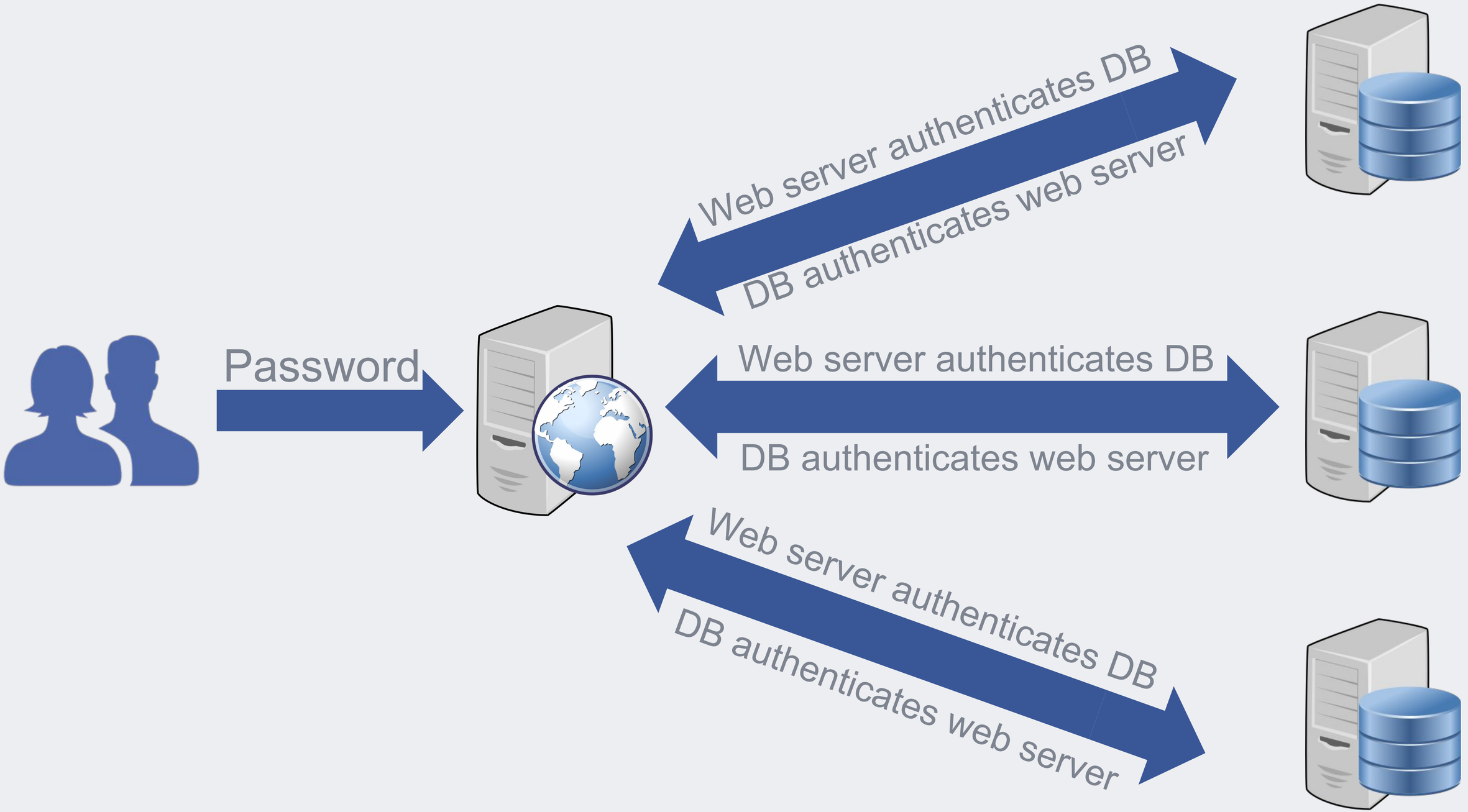
Every request needs a few things

- Log everything about the request
- Log the new cert
- Log where the new cert went

Benefits

What do we get?

- Authentication of both sides of a connection
- Authorization based on many attributes
- Accounting
- authnz is stateless


Password
Web server authenticates DB
DB authenticates web server
Web server authenticates DB
DB authenticates web server
Web server authenticates DB
DB authenticates web server

You don’t need to be Facebook!

- You can benefit from having an X.509 setup at any scale
- Hardcoded passwords between services are done with
- X.509 is useful outside of TLS

Final Tips

- Be serious about protecting your CA!
- Have a process to rotate your CA when the need arises
- Use unique serial numbers
- Be aggressive about eliminating users/passwords in code

facebook