cryptdomainmgr

automating Cert, TLSA, DKIM and many more

Stefan Helmert

Chaostreff Chemnitz

29. April 2018

Content

Motivation

fine

not so fine

Basics

SSL Certifcate

TLSA

DNSSEC

DKIM

Solution

cryptdomainmgr

Motivation

→ **let's make a web app** ←

- DNS
- Webpage
- E-Mail
- Mailinglist
- **and the s for security**

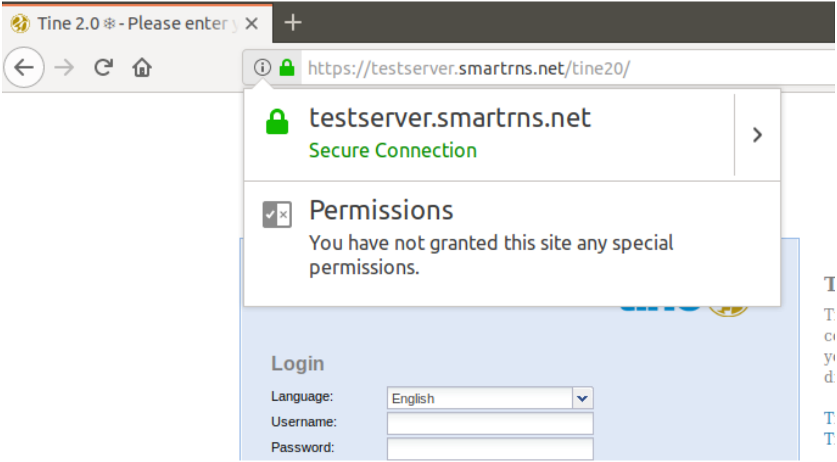
DeMotivation

→ let's make a web app ←

- DNS
  - SOA
  - DNSSEC
- Webpage
  - HTTPS
  - Certificate
  - HSTS
  - SRV
  - TLSA
- E-Mail
  - Spam
  - DKIM
  - SPF
  - ADSP
  - DMARC
  - SRV
- Mailinglist
  - SRS

DeMotivation

fine



Tine 2.0 - Please enter

https://testserver.smartrns.net/tine20/

testserver.smartrns.net

Secure Connection

Permissions

You have not granted this site any special permissions.

Login

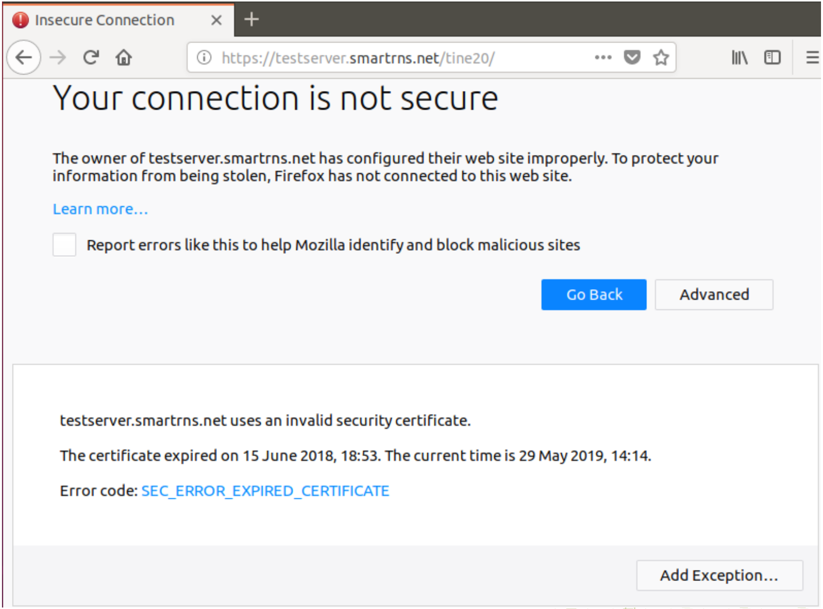
Language: English

Username:

Password:

DeMotivation

not so fine



Your connection is not secure

The owner of testserver.smartrns.net has configured their web site improperly. To protect your information from being stolen, Firefox has not connected to this web site.

Learn more…

□ Report errors like this to help Mozilla identify and block malicious sites

Go Back Advanced

testserver.smartrns.net uses an invalid security certificate.

The certificate expired on 15 June 2018, 18:53. The current time is 29 May 2019, 14:14.

Error code: SEC_ERROR_EXPIRED_CERTIFICATE

Add Exception…

Basics

SSL Certifcate

- authentication (phishing)
- integrity (man in the middle)
- privacy (spy)

→ certbot renew

Basics

TLSA

DANE – DNS-based Authentication of Named Entities
Transport Layer Security Authentication

- locks certificate to domain/DNS (fraudulent CA, stolen cert)

→ to do

Basics

DNSSEC

Domain Name System Security Extensions

- authenticate domain owner
- integrity (DNS cache poisoning)

→ done by domain provider

Basics

DKIM

DomainKeys Identified Mail

- authenticate MTA (fake/spam server)
- integrity (man in the middle)

→ to do

autorenew

- prepare
  - generate certificate
  - calculate TLSA from certificate
  - add TLSA RR
  - generate key pair for DKIM
  - calculate DKIM
  - add DKIM RR
- rollover
  - use new certificate
  - use new DKIM key
- cleanup
  - remove old TLSA RR
  - remove old DKIM RR
  - delete old certificates
  - delete old DKIM keys