cryptdomainmgr

automating Cert, TLSA, DKIM and many more

Stefan Helmert

Chaostreff Chemnitz

9. Mai 2018

Content

Motivation

→ **let's make a web app** ←

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

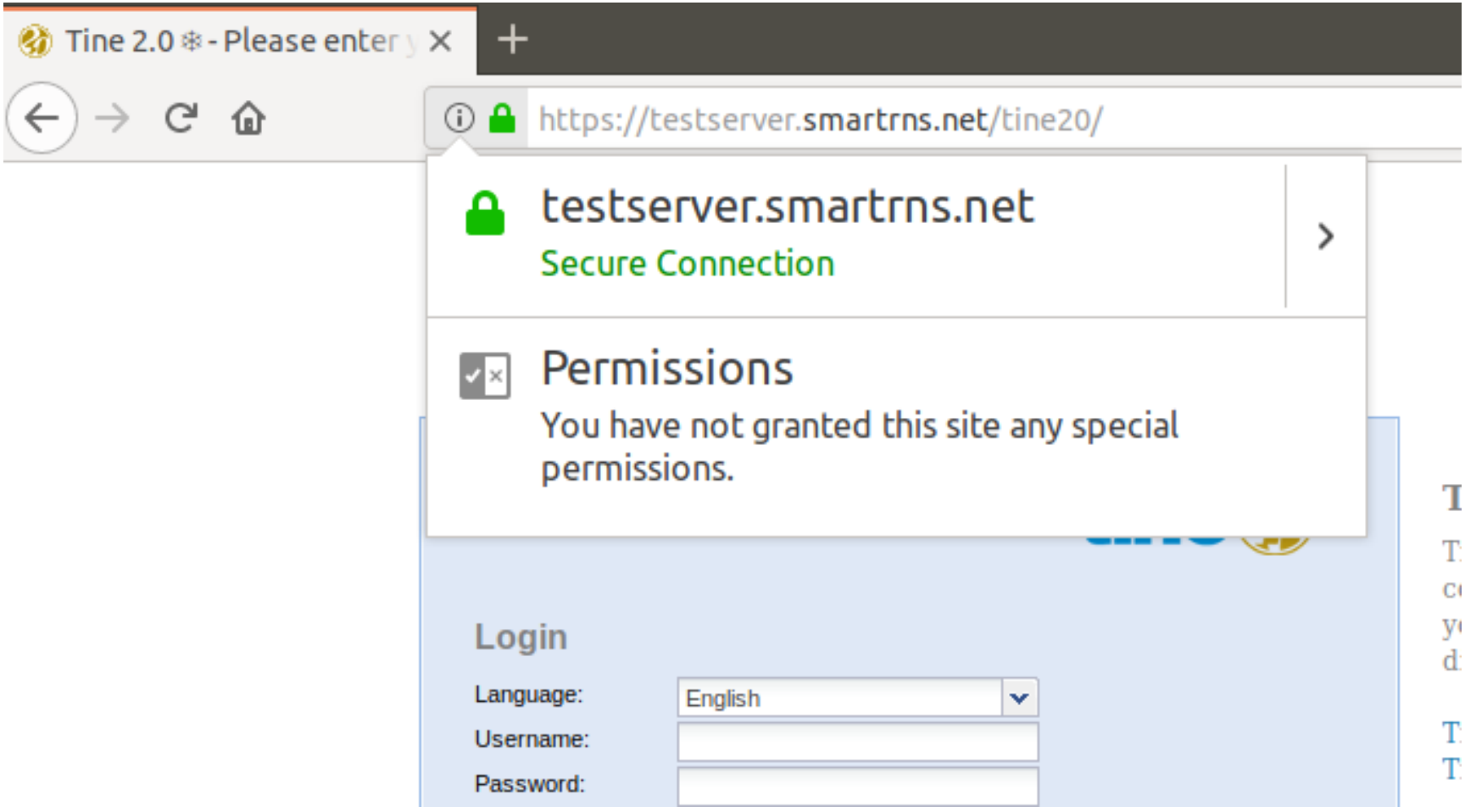
DeMotivation

→ **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

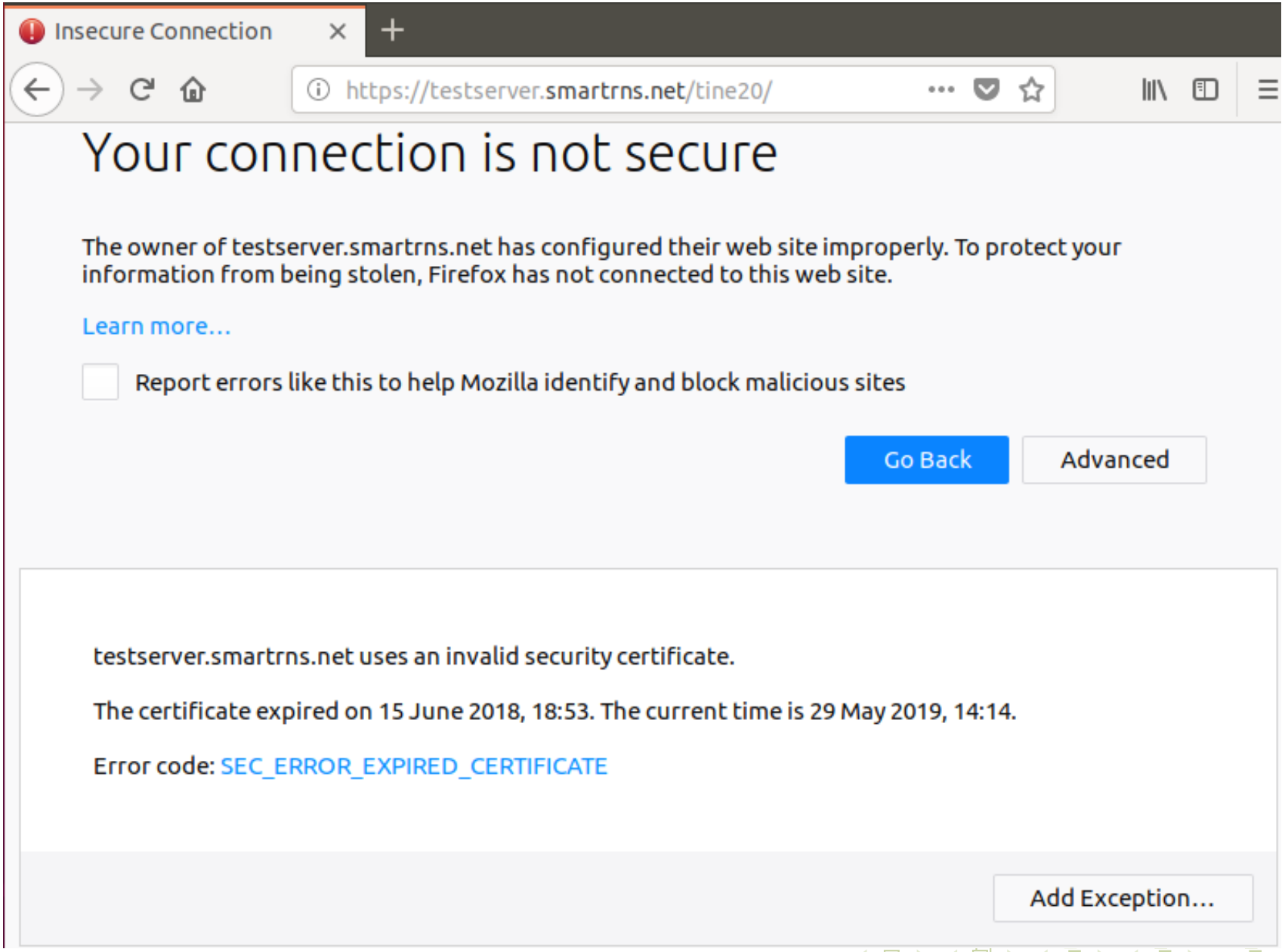
DeMotivation

fine



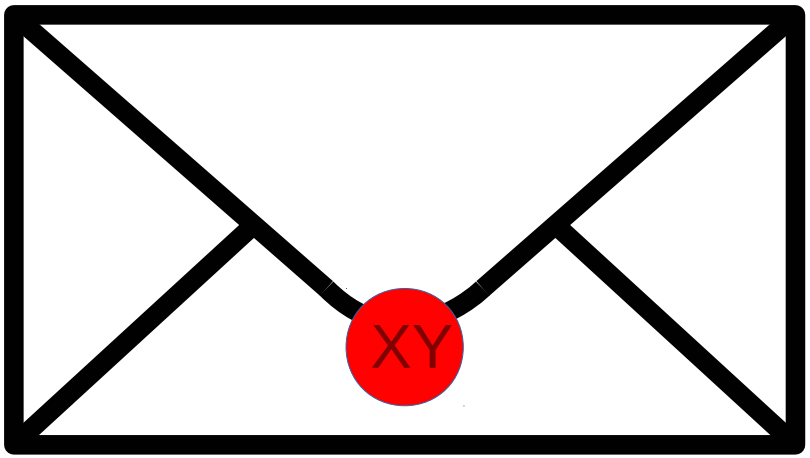
DeMotivation

not so fine



Basics

SSL Certifcate



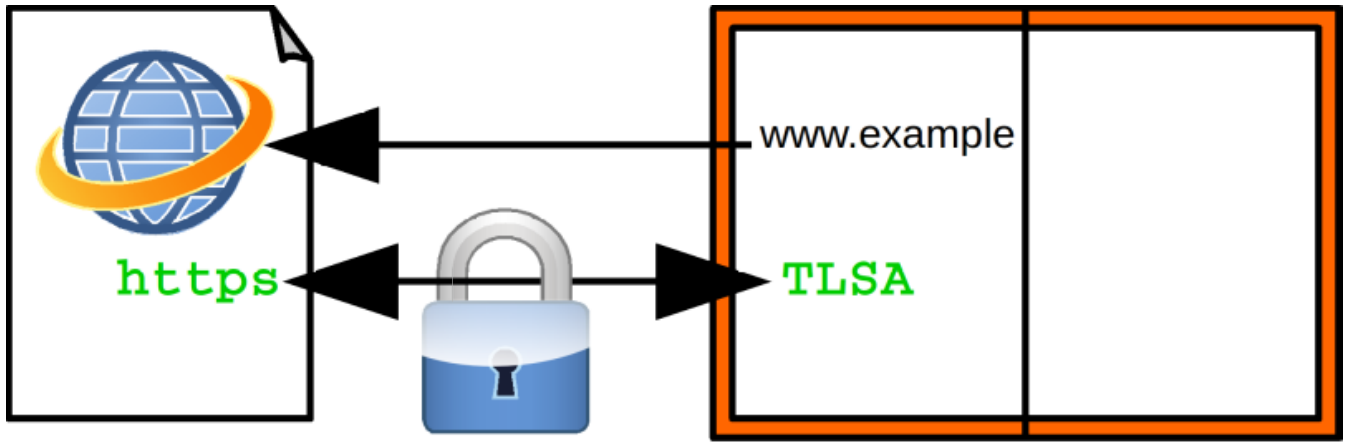
- authentication (phishing)
- integrity (man in the middle)
- privacy (spy)

$\rightarrow$ certbot renew

Basics

TLSA

DANE – DNS-based Authentication of Named Entities



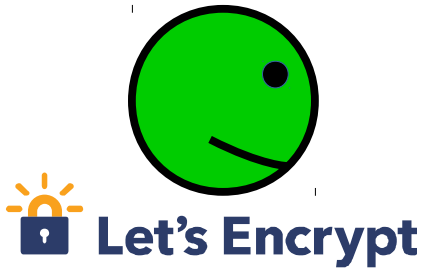
TLSA – Transport Layer Security Authentication

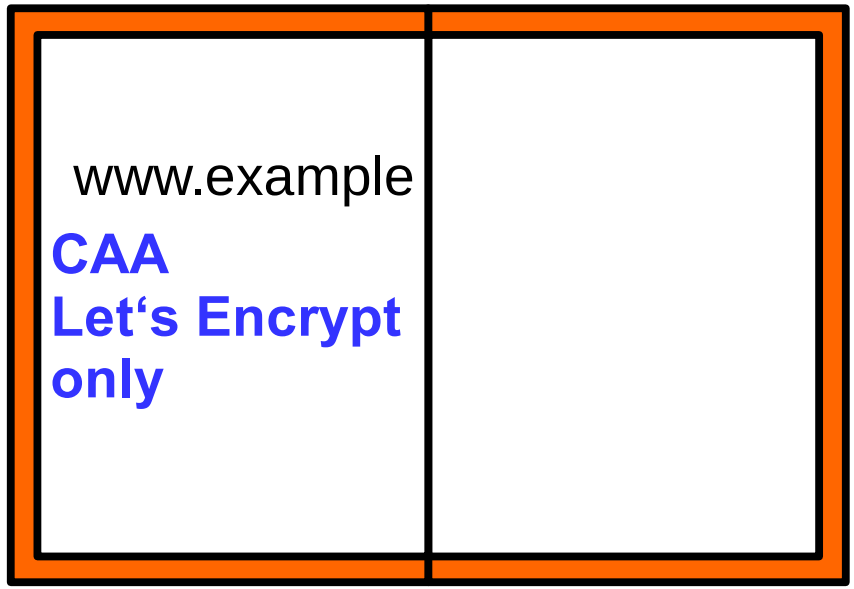
- locks certificate to domain/DNS (fraudulent CA, stolen cert)

→ to do

Basics

CAA



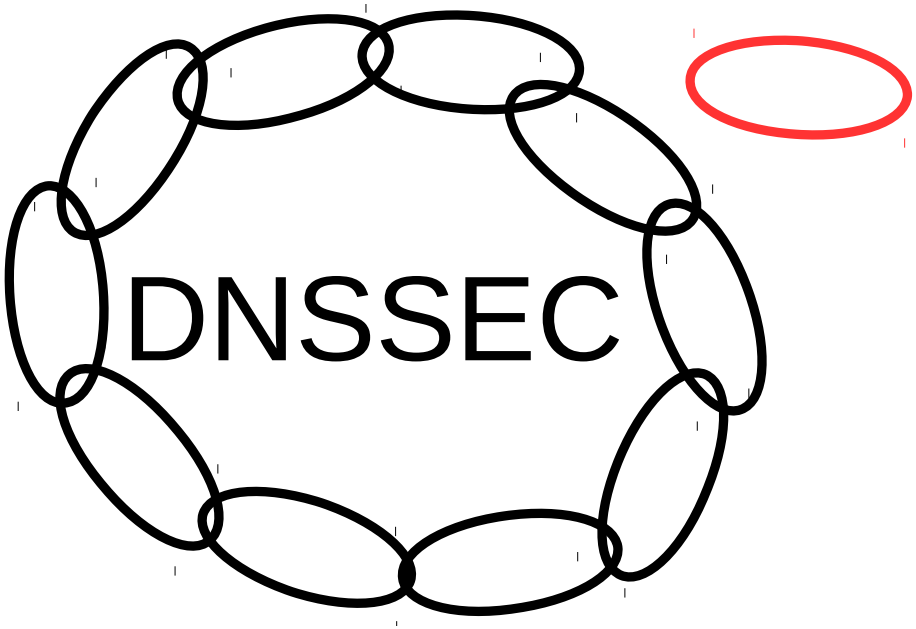


CAA – Certification Authority Authorization

- specifies allowed CA
- checked by CA

Basics

DNSSEC



Domain Name System Security Extensions

- authenticate domain owner
- integrity (DNS cache poisoning)

$\rightarrow$ done by domain provider

Basics

DKIM

DomainKeys Identified Mail

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

→ to do

Basics

additional DNS records

SPF – Sender Policy Framework

- which server is allowed to send email

ADSP – Author Domain Signing Practices

- defines, if email must be DKIM signed

DMARC – Domain-based Message Authentication, Reporting and Conformance

- successor of SPF and ADSP
- overrides SPF and ADSP
- additional parameters: report email

SRV – Service

- announces services

Cryptdomainmgr

autorenew process

- 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

Cryptdomainmgr

structure

- cryptdomainmgr
  - dnsuptools
    - domrobot
  - certbot

Cryptdomainmgr

update cycle

update – set a, aaaa, srv, dmarc, spf, adsp

```
~/cryptdomainmgr$ ./update.py inwxcred.conf example.conf
```

prepare cycle – generate Cert, TLSA, DKIM

```
~/cryptdomainmgr$ ./prepare.py inwxcred.conf example.conf
```

rollover cycle – use Cert, TLSA, DKIM

```
~/cryptdomainmgr$ ./rollover.py inwxcred.conf example.conf
```

cleanup cycle – remove outdated

```
~/cryptdomainmgr$ ./cleanup.py inwxcred.conf example.conf
```

Configuration

DNS credential

```
~/cryptdomainmgr$ cat inwxcred.conf

[domain]
user = myusername
passwd = mypassword
```

Configuration

Certificates

```
~/cryptdomainmgr$ cat example.conf

[certificate]
generator = certbot
email = stefan.helmert@t-online.de
keysize = 4096

[certificate:maincert]
destination = /etc/ssl
extraflags = --staging, --renew-with-new-domains, --hsts
certname = fullchain.pem
```

- multiple domains using `maincert` → SAN certificate

Configuration

DKIM

```
~/cryptdomainmgr$ cat example.conf

[dkim]
generator = rspamd

[dkim:maindkim]
signingConfTemplateFile = ~/cryptdomainmgr/dkim_signing_ter
signingConfTemporaryFile = /etc/rspamd/dkim_signing_new.cor
signingConfDestinationFile = /etc/rspamd/local.d/dkim_signi
```

Configuration

Domain

```
~/cryptdomainmgr$ cat example.conf

[domain]
user = myusername
handler = dnsuptools

[domain:domain.example]
soa.hostmaster = stefan.helmert@t-online.de
soa.refresh = 7200

[domain:sub.domain.example]
ip4 = auto, 192.168.0.1
ip6+ = auto, 0ffc::0030
mx = mail20.domain.example:20, mail30.domain.example:30
mx.40 = mail40.domain.example, mail50.domain.example:50
mx.10+= mail10.domain.example
```

Configuration

Domain

set A record

```
~/cryptdomainmgr$ cat example.conf

[domain:sub.domain.example]
ip4 = auto, 192.168.0.1
```

means:

- add external ip and `192.168.0.1` to sub.domain.example
- delete all other A records of sub.domain.example

Configuration

Domain

add A record

```
~/cryptdomainmgr$ cat example.conf

[domain:sub.domain.example]
ip4+ = auto, 192.168.0.1
```

means:

- add external ip and `192.168.0.1` to sub.domain.example
- ~~delete all other A records of sub.domain.example~~

Configuration

Domain

set MX record

```
~/cryptdomainmgr$ cat example.conf

[domain:sub.domain.example]
mx = mail20.domain.example:20, mail30.domain.example:30
```

means:

- add MX records
  - mail20.domain.example with prio 20
  - mail30.domain.example with prio 30
- delete all other MX records from sub.domain.example

Configuration

Domain

set MX record

```
~/cryptdomainmgr$ cat example.conf

[domain:sub.domain.example]
mx.40 = mail40.domain.example, mail50.domain.example:50
```

means:

- add MX records
  - mail40.domain.example with prio 40
  - mail50.domain.example with prio 50
- delete all other MX records with prio 40 from sub.domain.example

Configuration

Domain

set SRV record

```
~/cryptdomainmgr$ cat example.conf

[domain:sub.domain.example]
srv.service.proto.port.weight.prio
= sub.domain.example:PRIO:WEIGHT:PORT:PROTO:SERVICE
```

Configuration

Domain

set DMARC entries

```
~/cryptdomainmgr$ cat example.conf

[domain:sub.domain.example]
dmarc.p = quarantine
dmarc.rua = mailto:stefan.helmert@t-online.de
dmarc.ruf = mailto:stefan.helmert@gmx.net
```

- changes the entries `p`, `rua`, `ruf` of the `DMARC` record
- entries `adkim`, `aspf`, `pct` do not change
- „atomic“ operation
- only one `DMARC` record allowed!

Configuration

Domain

set DMARC record

```
~/cryptdomainmgr$ cat example.conf

[domain:sub.domain.example]
dmarc =
dmarc.p = quarantine
dmarc.rua = mailto:stefan.helmert@t-online.de
dmarc.ruf = mailto:stefan.helmert@gmx.net
```

- changes the entries `p`, `rua`, `ruf` of the `DMARC` record
- remove all other entries of this record
- „atomic“ operation
- at most one `DMARC` record allowed!

Configuration

Domain

set SOA entries

```
~/cryptdomainmgr$ cat example.conf

[domain:domain.example]
soa.hostmaster = stefan.helmert@t-online.de
soa.refresh = 7200
```

- changes the entries `hostmaster`, `refresh` of the `SOA` record
- `primns`, `serial`, `retry`, `expire`, `ncttl` not changed
- „atomic“ operation
- exact one `SOA` record in top level allowed!

Configuration

Domain

set SPF flags

```
~/cryptdomainmgr$ cat example.conf

[domain:domain.example]
spf = -mx, a, ?all, +aaaa
```

- add given flags to SPF record
- remove all other flags from SPF record
- „atomic“ operation
- at most one SPF record is allowed!

Configuration

Domain

set ADSP and CAA records

```
~/cryptdomainmgr$ cat example.conf

[domain:domain.example]
adsp = all
caa =   0 issue letsdecrypt.org,
      128 issuewild examplecert.example
```

- atomic update ADSP record
- add the CAA records
- remove all other CAA records

Configuration

Domain

combine stuff – TLSA and DKIM

```
~/cryptdomainmgr$ cat example.conf

[domain:sub.domain.example]
tlsa = 3 0 1, 3 1 1
certificate = maincert
dkim = maindkim
```

prepare cycle

- add `TLSA` and `DKIM` records

rollover cycle

- no DNS changes
- apply certificates and keys on server

cleanup cycle

- add `TLSA` and `DKIM` records (again)
- remove all other `TLSA` and `DKIM` records

Implementation

cryptdomainmgr

cryptdomainmgr.py	core, brings everything together
cdmconfighandler.py	reads/interpretes config (ini) files
update.py	command line interface for generic DNS update
prepare.py	command line interface for prepare cycle
rollover.py	command line interface for rollover cycle
cleanup.py	command line interface for cleanup cycle
simplelogger/	logging abstraction, password $\rightarrow$ *****
dnsuptools/	domrobot interface abstraction, TLSA, DKIM calculation

Implementation

simplelogger

simplelogger.py core, produces output

deepops.py deep dict/list operations, password $\rightarrow$ *****

Implementation

dnsuptools

dnsuptools.py core, high level, record change & query methods

dnsupdate.py interface to domrobot, low level

dkimrecgen.py reads/interpretes dkim key file

tlsarecgen.py reads/interpretes certificate file

simplelogger/ see simplelogger 2

inwxclient/ domrobot client

Discussion

???