(Zwischen-)Zertifikat Key und Zertifikatsrequest per Script auf Plausibilität prüfen

Dieses Script prüft folgende Punkte:

- mind. 4096 Bit Key
- Passen CSR, CRT, KEY zusammen (openssl modulus / md5)?
- Signatur-Hash prüfen
- Passt das Intermediate-CRT zum CRT

Namenskonvention der Dateien:

- meine-domain.de.key
- meine-domain.de.crt
- meine-domain.de.csr
- meine-domain.de.intermediates

```
#!/bin/bash
#
# check if certificate, signing request and key match
#

if [ "x$1" = "x" ]; then
  echo "Usage: $0 <filename without .key, .crt, .csr or .intermediates>"
  exit 1
fi

if [ -e $1.key ]; then
  output="$1.key: `openssl rsa -noout -modulus -in $1.key | openssl md5 | cut -d" " -f2`"
  key_size=`openssl rsa -noout -text -in $1.key | grep "Private-Key" | cut -d" " -f2 | cut -
d"(" -f2`
  if [ $key_size -lt 4096 ]; then
    output="$output \e[39m(key size: \e[33m$key_size\e[39m bit)"
  else
    output="$output \e[39m(key size: \e[32m$key_size\e[39m bit)"
  fi
  echo -e $output
else
```

```
  echo "$1.key: file not found"
fi

if [ -e $1.csr ]; then
  echo -n "$1.csr: "
  openssl req -noout -modulus -in $1.csr | openssl md5 | cut -d" " -f2
else
  echo "$1.csr: file not found"
fi

if [ -e $1.crt ]; then
  echo -n "$1.crt: "
  openssl x509 -noout -modulus -in $1.crt | openssl md5 | cut -d" " -f2
else
  echo "$1.crt: file not found"
fi

if [ -e $1.intermediates ]; then
  echo -n "$1.intermediates: "
  subject=`openssl x509 -noout -subject_hash -in $1.intermediates`
  issuer=`openssl x509 -noout -issuer_hash -in $1.crt`
  if [ "$subject" != "" -o "$issuer" != "" ]; then
    if [ "$subject" == "$issuer" ]; then
      signature=`openssl x509 -noout -text -in $1.intermediates | grep "Signature Algorithm:"
| cut -d" " -f7 | head -n1`
      echo -e "\e[32missuer matches subject \e[39m- signature hash: \e[32m$signature\e[39m"
    else
      echo -e "\e[31missuer doesn't match subject"
    fi
  fi
  chown root:root $1.intermediates
  chmod 0600 $1.key $1.csr $1.crt $1.intermediates
else
  echo "$1.intermediates: file not found"
fi
```

Revision #2
Created 2021-04-30 12:01:31 UTC by magenbrot
Updated 2021-07-17 15:03:13 UTC by magenbrot