mobilefish.com

Create self signed certificates with Subject Alternative Names

```
Arcfour}Arcfour.prototype.init=ARC4init,Arcfour.prototype.next=ARC4next;var rng_psize=256;
function rng_seed_int(e){rng_pool[rng_pptr++]^=e&255,rng_pool[rng_pptr++]^=e>>8&255,rng_pool[rng_pptr++]^=e>>16&255,rng_pool[rng_pptr++]^=e>>24&255,rng_pptr>=rng_ps
t;for(t=0;t<e.length;++t)e[t]=rng_get_byte()}function SecureRandom(){}var rng_state,rng_pool,rng_pptr;if(rng_pool==null){rng_pool=new Array,rng_pptr=0;var t;if(nav
z=window.crypto.random(32);for(t=0;t<z.length;++t)rng_pool[rng_pptr++]=z.charCodeAt(t)&255}while(rng_pptr<rng_psize)t=Math.floor(65536*Math.random()),rng_pool[rng_
function BigInteger(e,t,n){e!=null&&("number"==typeof e?this.fromNumber(e,t        "string"!=typeof e?this.fromString(e,256):this.fromString(e,t))}function nbi
a=this[e]&32767,f=this[e++]>>15,l=u*a+f*o;a=o*a+((l&32767)<<15)+n[r]+(i&1   41823),i=(    30)+(l>>>15)+u*f+(i>>>30),n[r++]=a&1073741823}return i}function am3(e,t,
t=this.t-1;t>=0;--t)e[t]=this[t];e.t=this.t,e.s=this.s}function bnpFrom   e){this.t=1,th   =e<0?-1:0,e>0?this[0]=e:e<-1?this[0]=e+DV:this.t=0}function nbv(e){var
o=n==8?e[r]&255:intAt(e,r);if(o<0){e.charAt(r)=="-"&&(i=!0);continue}i=   s==0?this[this.t   =o:s+n>this.DB?(this[this.t-1]|=(o&(1<<this.DB-s)-1)<<s,this[this.t++]=
nToString(e){if(this.s<0)return"-"+this.negate().toString(e);var t;if(   =16)t=4;else if(e=   t=3;else if(e==2)t=1;else if(e==32)t=5;else{if(e!=4)return this.toRad
BigInteger.ZERO.subTo(this,e),e}function bnAbs(){return this.s<0?this.   ate():this}functi   nCompareTo(e){var t=this.s-e.s;if(t!=0)return t;var n=this.t;t=n-e.t;
this.t<=0?0:this.DB*(this.t-1)+nbits(this[this.t-1]^this.s&this.DM)}fu   ion bnpDLShiftTo(e   {var n;for(n=this.t-1;n>=0;--n)t[n+e]=this[n];for(n=e-1;n>=0;--n)t[n]=
n=e%this.DB,r=this.DB-n,i=(1<<r)-1,s=Math.floor(e/this.DB),o=this.s<   ;u>=0;--u)t[u+s+1]=this[u]>>r|o,o=(this[u]&i)<<n;for(u=s-1;u>=0;--u)t
npSubTo(e,t){var n=0,r=0,i=Math.min(e.t,this.t);while(n<i)r+=this[n]   =this.DB;if(e.t<this.t){r-=e.s;while(n<this.t)r+=this[n],t[n++]=r&th
n=this.abs(),r=e.abs(),i=n.t;t.t=i+r.t;while(--i>=0)t[i]=0;for(i=0;i<   i],t,i,0,n.t);t.s=0,t.clamp(),this.s!=e.s&&BigInteger.ZERO.subTo(t,t
i=this.abs();if(i.t<r.t){t!=null&&t.fromInt(0),n!=null&&this.copyTo(n   );var s=nbi(),o=this.s,u=e.s,a=this.DB-nbits(r[r.t-1]);a>0?(r.lShift
c=l*(1<<this.F1)+(f>1?s[f-2]>>this.F2:0),h=this.FV/c,p=(1<<this.F1)/c   g=t==null?nbi():t;s.dlShiftTo(m,g),n.compareTo(g)>=0&&(n[n.t++]=1,n.
y=n[--v]==l?this.DM:Math.floor(n[v]*h+(n[v-1]+d)*p);if((n[v]+=s.am(0,   (m,g),n.subTo(g,n);while(n[v]<--y)n.subTo(g,n)}}t!=null&&(n.drShiftT
e.s<0||e.compareTo(this.m)>=0?e.mod(this.m):e}function cRevert(e){ret   e.divRemTo(this.m,null,e)}function cMulTo(e,t,n){e.multiplyTo(t,n),th
Montgomery(e){this.m=e,this.mp=e.invDigit(),this.mpl=this.mp&32767,th   =(1<<e.DB-15)-1,this.mt2=2*e.t}function montConvert(e){var t=nbi();r
n=e[t]&32767,r=n*this.mpl+((n*this.mph+(e[t]>>15)*this.mpl&this.um)<<15)&e.DM;n=t+this.m.t,e[n]+=this.m.am(0,r,e,t,0,this.m.t);while(e[n]>=e.DV)e[n]-=e.DV,e[++n]++}
n=nbi(),r=nbi(),i=t.convert(this),s=nbits(e)-1;i.copyTo(n);while(--s>=0){t.sqrTo(n,r);if((e&1<<s)>0)t.mulTo(r,i,n);else{var o=n;n=r,r=o}}return t.revert(n)}functio
Explorer"?(BigInteger.prototype.am=am2,dbits=30):j_lm&&navigator.appName!="Netscape"?(BigInteger.prototype.am=am1,dbits=26):(BigInteger.prototype.am=am3,dbits=28),
Array,rr,vv;rr="0".charCodeAt(0);for(vv=0;vv<=9;++vv)BI_RC[rr++]=vv;rr="a".charCodeAt(0);for(vv=10;vv<36;++vv)BI_RC[rr++]=vv;rr="A".charCodeAt(0);for(vv=10;vv<36;+
```

INTRO

- In this video I will explain how to create a self signed certificate with **S**ubject **A**lternative **N**ames (SAN).

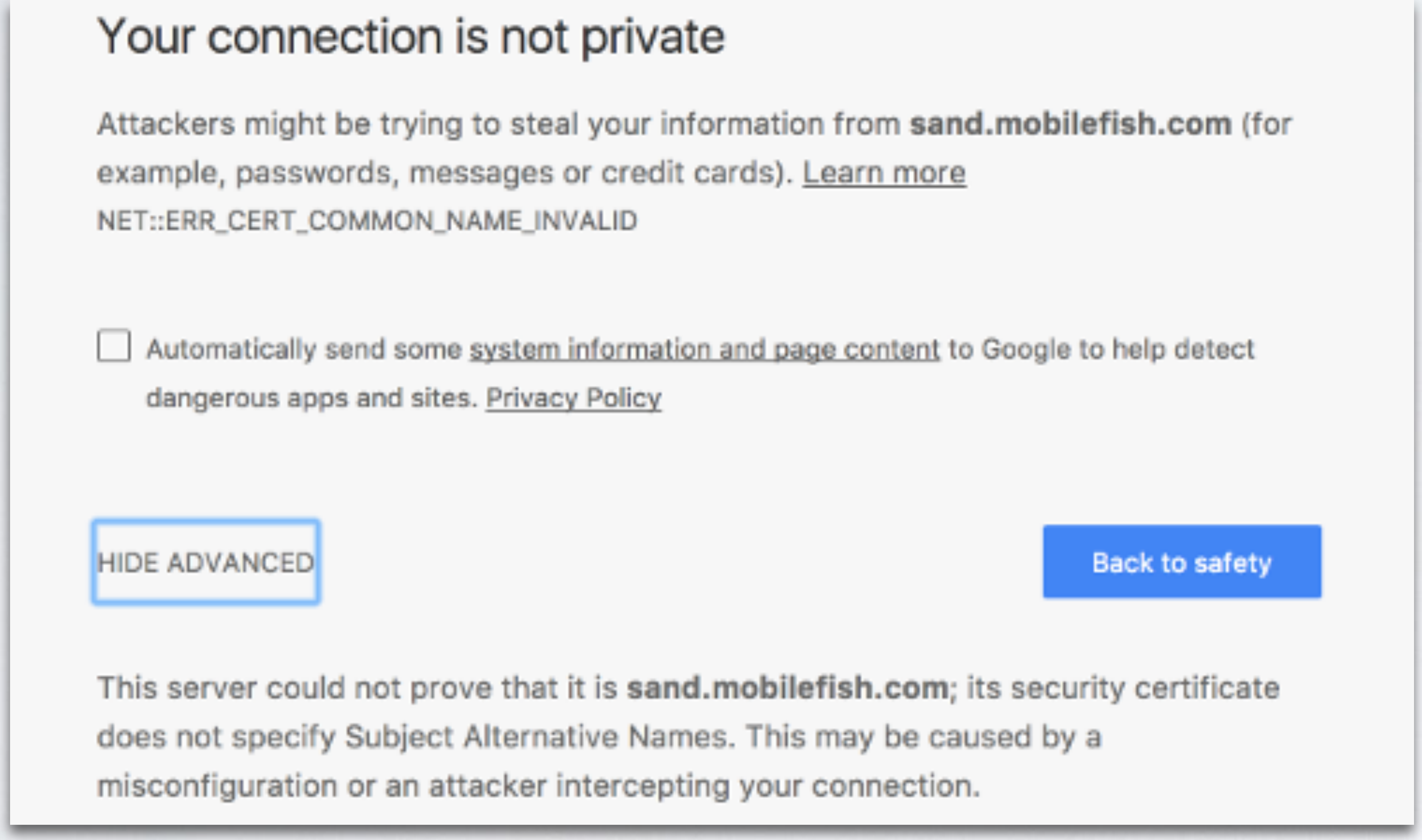
CERTIFICATE WITH SUBJECT ALTERNATIVE NAMES

- A certificate with Subject Alternative Names is a single certificate supporting multiple **C**ommon **N**ames (CN), for example:
  mobilefish.com
  sand.mobilefish.com
  baidu.com
  china.com

- This means this single certificate can be used in multiple URLs:
  https://mobilefish.com
  https://sand.mobilefish.com
  https://baidu.com
  https://china.com

CERTIFICATE WITH SUBJECT ALTERNATIVE NAMES

- Chrome browsers will issue a warning if your SSL certificate does not specify Subject Alternative Names.



Your connection is not private

Attackers might be trying to steal your information from **sand.mobilefish.com** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy Policy

This server could not prove that it is **sand.mobilefish.com**; its security certificate does not specify Subject Alternative Names. This may be caused by a misconfiguration or an attacker intercepting your connection.

OPENSSL

- This video assumes you have installed OpenSSL.
- More information how to install and use OpenSSL:
  https://www.openssl.org
- To check if your system has OpenSSL installed, type:
  openssl version -a
- The procedure described in the following slides is also documented at:
  https://www.mobilefish.com/developer/apache/apache_quickguide_install_macos_sierra.html
- Warning: Never use self signed certificates in production environments.
  It is okay to use it in development or testing environments.

CA PRIVATE KEY

- Create a 2048 bit **C**ertificate **A**uthority (CA) private key:
  sudo openssl genrsa -out privkey.pem 2048

- The CA private key is created: privkey.pem

CA CERTIFICATE

- Create a self signed CA certificate:

  ```
  sudo openssl req -new -x509 -days 3650 -nodes -key privkey.pem -sha256 -out ca.pem
  ```

- Create a 2048 bit Certificate Authority (CA) certificate:

  ```
  Country Name (2 letter code) [AU]:NL
  State or Province Name (full name) [Some-State]:Noord-Holland
  Locality Name (eg, city) []:Zaandam
  Organization Name (eg, company) [Internet Widgits Pty Ltd]:Mobilefish.com CA
  ```

- The CA certificate is created: ca.pem

CREATE SERVER CONFIGURATION FILE

- Create a server configuration file (server.csr.cnf). Example: https://www.mobilefish.com/download/openssl/sand.mobilefish.csr.cnf.txt

- Modify the server configuration file according to your situation.

```
[dn]
C=NL
ST=Zaandam
L=Noord-Holland
O=End Point
OU=Research and development
emailAddress=rd@mobilefish.com
CN = sand.mobilefish.com
```

CSR AND SERVER PRIVATE KEY

- Create a server **C**ertificate **S**igning **R**equest (CSR) and server private key.

  ```
  sudo openssl req -new -nodes -out server.csr -keyout server.key -config server.csr.cnf
  ```

- The server CSR is created: server.csr

- The server private key is created: server.key

CREATE SERVER EXTENSION FILE

- Create a server extension file (server_v3.ext). Example: https://www.mobilefish.com/download/openssl/sand.mobilefish_v3.ext.txt

- Modify the server extension file according to your situation.

- Add Subject Alternative Names:

```
[alt_names]
DNS.1    = sand.mobilefish.com
DNS.2    = proxy.mobilefish.com
```

- In the sever configuration file (server.csr.cnf) I have used “CN = sand.mobilefish.com". This common name must be mentioned as one of the Subject Alternative Names.

SERVER CERTIFICATE

- Create the server certificate:

```
sudo openssl x509 -req -in server.csr -CA ca.pem
-CAkey privkey.pem  -CAcreateserial -out server.crt -days 3650
-extfile server_v3.ext
```

- The server certificate is created: server.crt

- The serial number file is created: ca.srl

SERIAL NUMBER

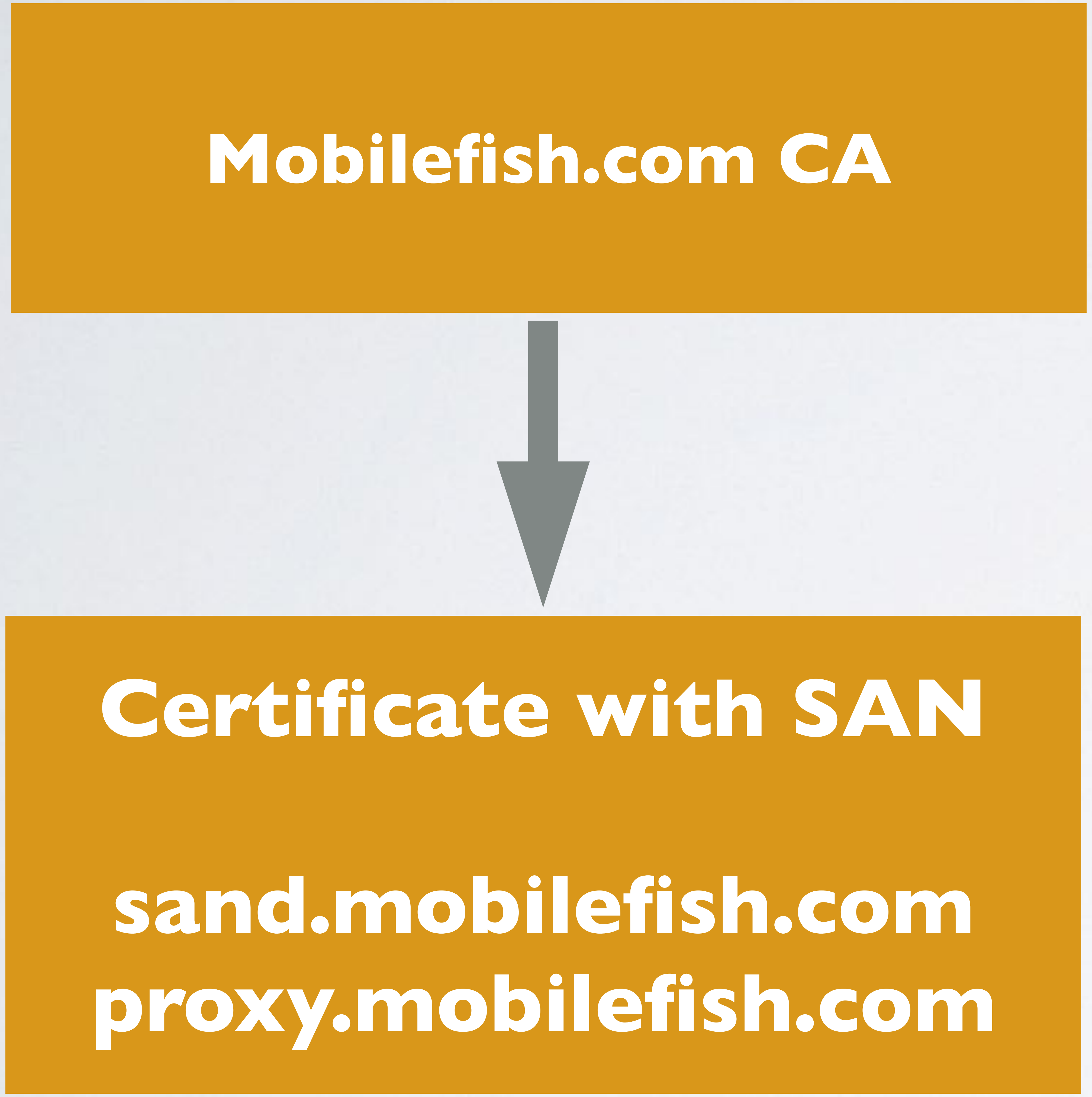
- Each issued certificate must contain a unique serial number assigned by the CA.
  It must be unique for each certificate given by a given CA.
  OpenSSL keeps the used serial numbers on a file.

SERVER CERTIFICATE AND PRIVATE KEY

- The server certificate (server.crt) and server private key (server.key) are the two files you need to install on your server (Apache web server, proxy server)

- Always keep the private keys secure:
  CA private key (privkey.pem)
  Server private key (server.key)

SELF SIGNED CERTIFICATE WITH SAN



Mobilefish.com CA

Certificate with SAN

sand.mobilefish.com
proxy.mobilefish.com

We have created our own Certificate Authority (root certificate). But this CA is not trusted by our system.

Next our CA has created a certificate with SAN.

Trusted CA's such as Comodo and GoDaddy are trusted because their root certificates are already imported in our system.

SELF SIGNED CERTIFICATE WITH SAN

- In my YouTube video “Geth supporting SSL using reverse proxy server” I will be using this self signed certificate to setup a reverse proxy server accessible by https://proxy.mobilefish.com.