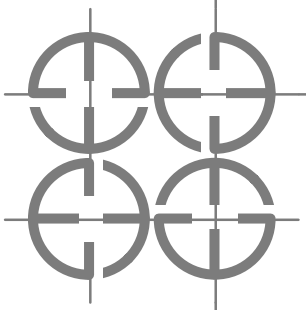


Web Weaving

Janvossensteeg 37
2312 WC Leiden
The Netherlands

Exporting Public key from HSM as X9.62

Apple and Google require a X9.62 style key for GAEN. The HIM its current PKCS#11 implementation does not seem to support ECDSA keys[1] export. The proprietary `cxitool` outputs the public key as a 65 byte hex blob.

With that blob an ASN1 X9.62 can be constructed by taking the ASN1 of the algorithm identifier (id-ecPublicKey0 and parameter (secp256r1) and postfixing this by the public key (as the length is known already).

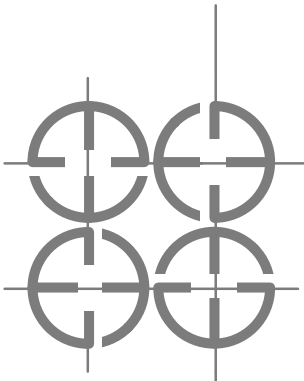
```
cxitool Dev=<hsmport>}@<hsmhost> \
        LogonPass=USR_<userid>,<pin> \
        Group=SLOT_<slotid> Spec=<specid> \
        ExportPubKeyFile=/tmp/ec.$$

(
        echo -----BEGIN PUBLIC KEY-----
        (
                #construct prefix
                openssl ecparam -name secp256r1 -genkey -noout | \
                        openssl ec -pubout  | tail +2 | head -2 |\
                        base64 -d  | xxd -p -l 26
                # extract key
                PUB=`tail -1 /tmp/ec.$$ | sed -e 's/.*PUB=//'`
        ) | xxd -r -p | base64
        echo -----END PUBLIC KEY-----
) | openssl ec -pubin > /etc/keys/ecdsa.pem

openssl ec -text -pubin < /etc/keys/ecdsa.pem

# This rm is fairly crucial - as cxitool will silently fail on the next
# run (but still having changed the key - so they are now out of sync).
rm -f /tmp/ec.$$
```

[1] The various export operations yields a truncated key. Cause unclear



About WebWeaving

WebWeaving has offered hands-on specialist consultancy and internet engineering. Since 1994 we have helped startups and large companies scale on the internet, drawing from a large network of technical experts. Scale not just in terms of hardware and bandwidth; but also scale in terms of staff and the organisational capability to continuously release and refine its products and software efficiently, timely and predictably. We help organisations understand the software life cycle and the total cost of ownership (including that of open source) relative to their ambitions.