Sign Apple mobileconfig files

`.mobileconfig` files

Configuration of mobile Apple devices such as the iPad and iPhone can be done using pre-cooked configuration files. These files are generated by the iPhone Configuration Utility (iPCU), which spits out an XML file with the extension `.mobileconfig`. Such a file can then be put up a web site so that users can download it to apply a certain so-called *profile*, which will be listed in the Settings/General panel on the device. Sometimes this is the only way to configure certain features, because the device's interface won't let you. A good example is Eduroam wireless networking with TTLS.

Deploying your profiles

There are three options to deploy your profile:

Unsigned

This is done when you export your profile using security **None**. When users try to install such a profile, they receive a red **Unsigned** warning, to warn that the content of the profile could have been tampered with. Fair enough.

Default signature

Happens when you select **Sign configuration profile** during export. This protect against tampering with the profile, but it still display a red **Not Verified**. That is because the signature is made with a self-signed certificate from the iPCU.

TCS (real) signature

This option involves adding a TCS personal signature to a profile, which will result in no warnings at all during installation by end users.

Because there is no option in the iPCU to use a specific certificate, we are going to use OpenSSL.

1. Create a profile with the iPCU and export it with security **None**. Make sure you have available the following files:

`visser@terena.org.key.pem`	The private key of your TCS personal certificate
`visser@terena.org.crt.pem`	The issued certificate
`personal_chain.pem`	File containing intermediate CAs

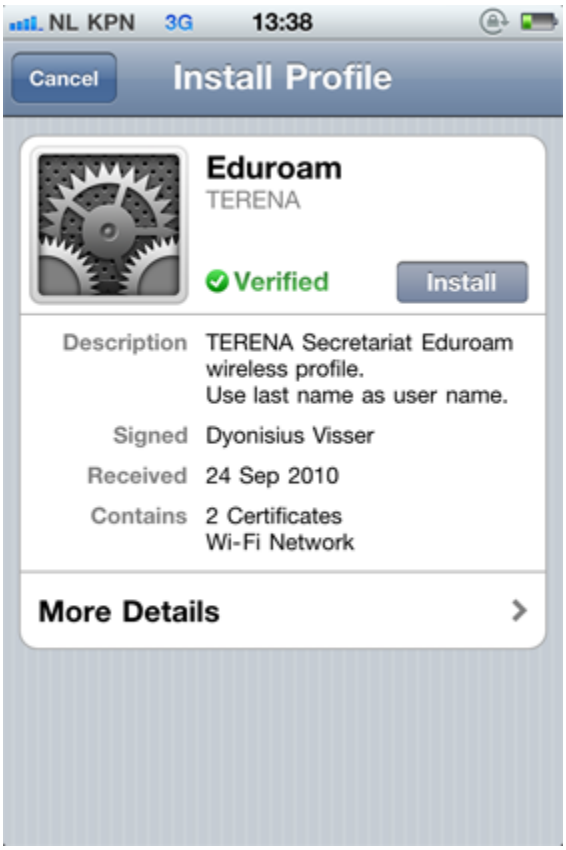
2. Add a signature:

```
openssl smime \
 -sign \
 -signer visser@terena.org.crt.pem \
 -inkey visser@terena.org.key.pem \
 -certfile personal_chain.pem \
 -nodetach \
 -outform der \
 -in MyProfile.mobileconfig \
 -out Myprofile_signed.mobileconfig
```

   The `-certfile` option is a bit tricky: if you do not use it, the signature will not contain any actual intermediate CAs.
   However, when you are online, the profile will still look verified. Very shortly after switching to Airplane Mode the profile becomes **Not Verified**.
   The only logical explanation is that the system gets the issuer certificate from the embedded URL in the signature:

content of `personal_chain.pem`	result
nothing (don't use it)	**Verified** when online, **Not Verified** when offline
TERENA Personal CA	Always **Verified**
TERENA Personal CA UTN-USERFirst-Client Authentication and Email AddTrust External CA Root AAA Certificate Services	Always **Verified**

   While it is theoretically enough to only include `TERENA Personal CA`, it is probably better for compatibility to add them all.
3. Put this mobileconfig on a website, and click it from Safari. You will be presented with a nice 'green' message:



You can see that the signing certificate was issued by TERENA Personal CA.