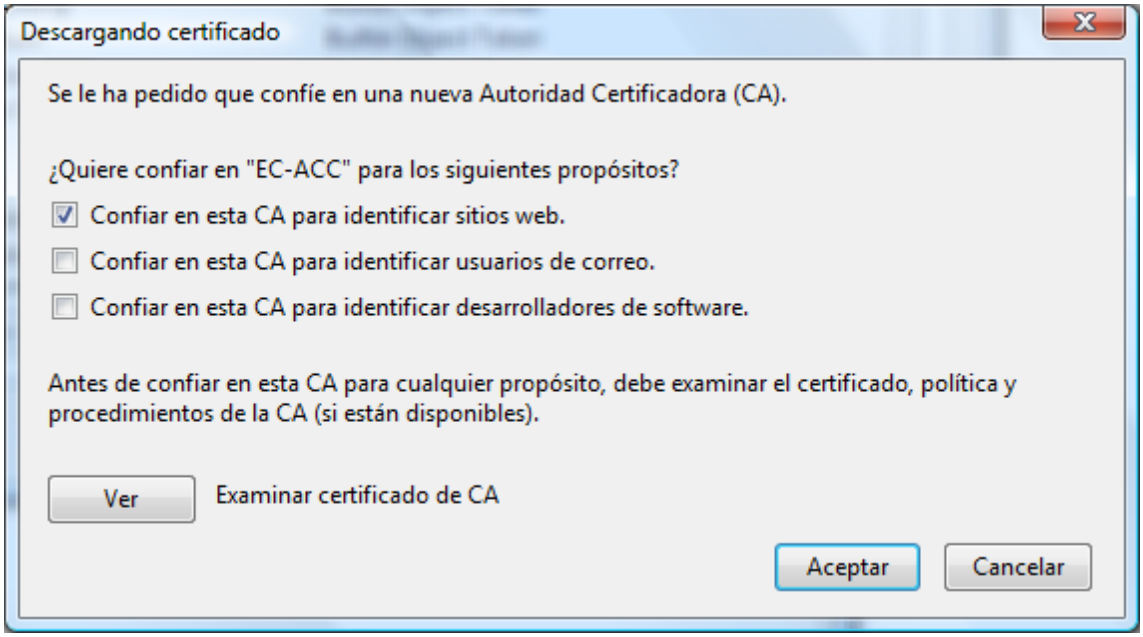
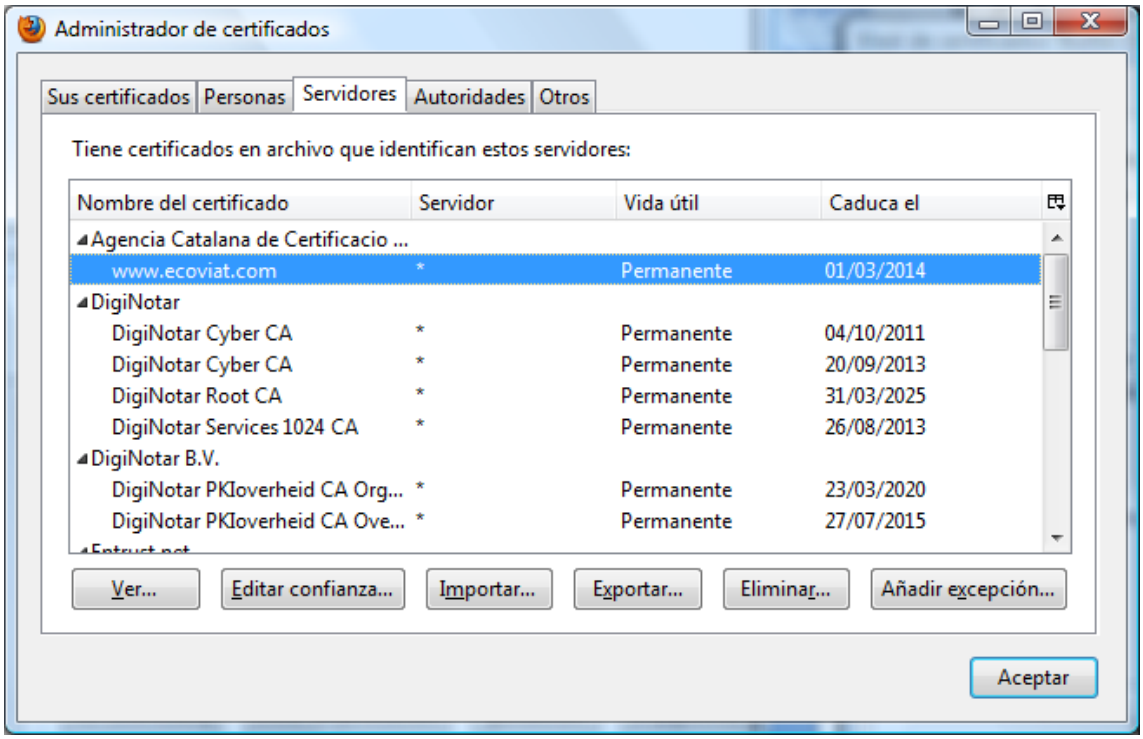
TEST OF CERTIFICATION CHAIN CONSTRUCTION IN FIREFOX WITH CATCERT SHA-256 HIERARCHY:

1. Go to %APPDATA%\Mozilla\Firefox\Profiles\
2. Move cert8.db to another directory
3. Restart Firefox
4. Import the root certificate EC-ACC SHA-256 with turned on the websites trust bit

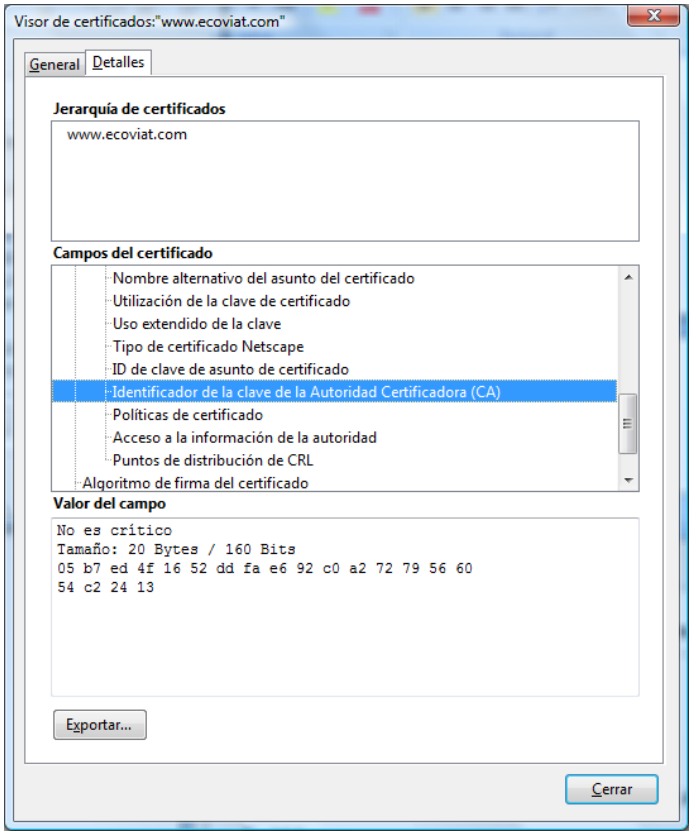


5. Import the intermediate certificate EC-GENCAT SHA-256
6. Import the intermediate certificate EC-SAFP SHA-256

7. At the “servers” tab import the certificate www.ecoviat.com



Finally: the certificate chain is not constructed:

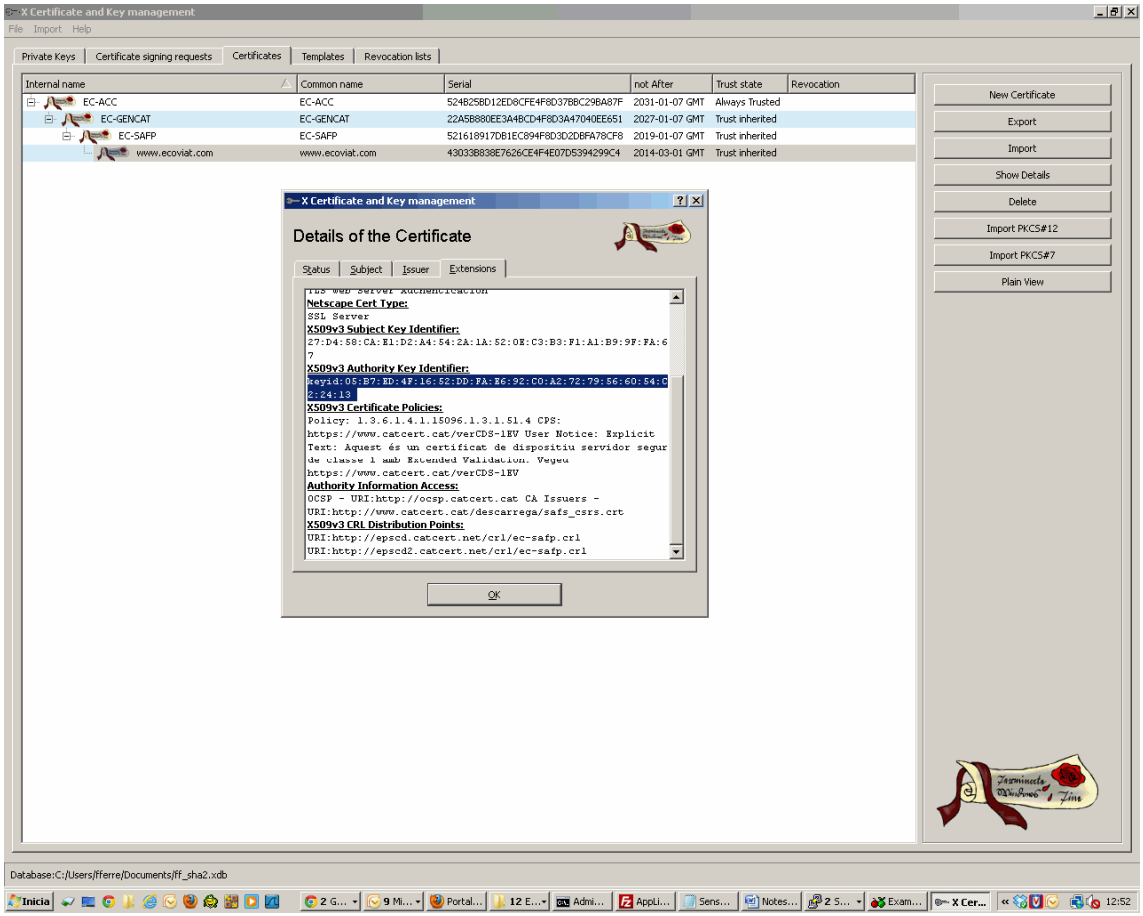


Then we have tested the same with the SHA-1 hierarchy and the chain is constructed correctly as expected.

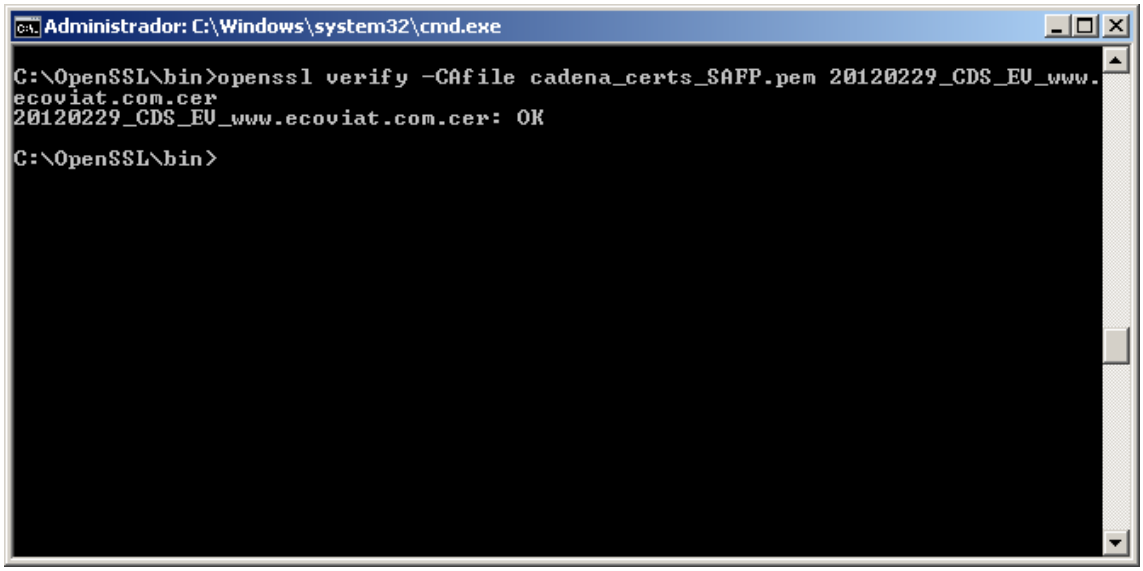
TESTS WITH OTHER SYSTEMS:

The chain SHA-256 is constructed without problems:

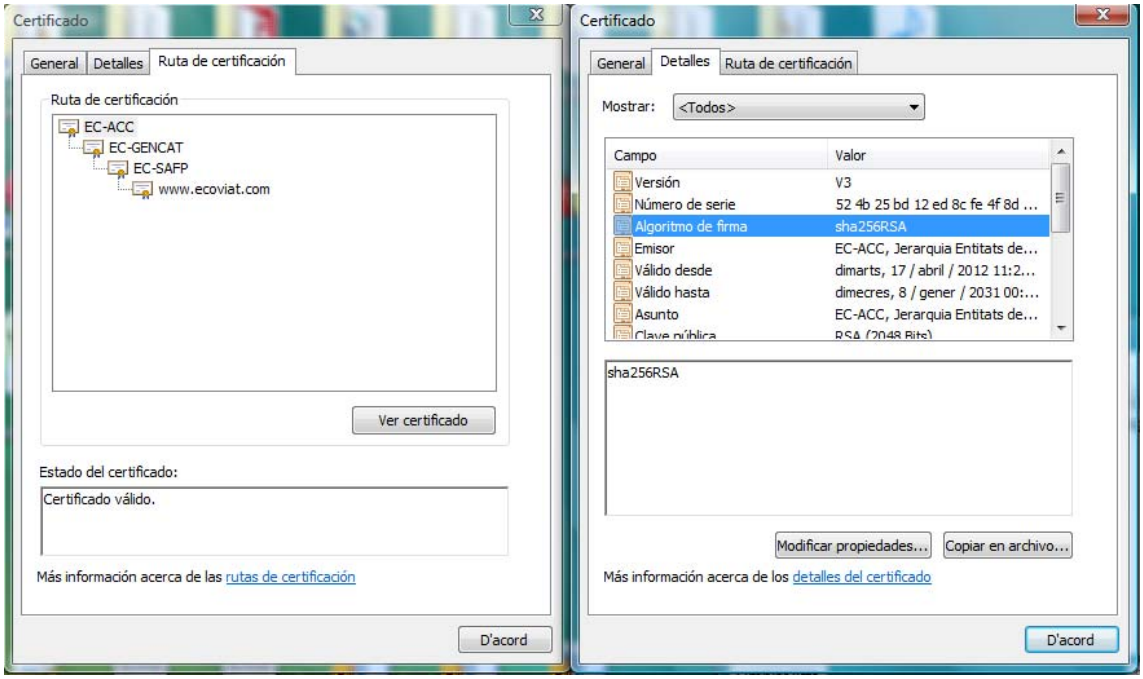
- With **XCA**:



- With the command **OpenSSL verify:**



- **With Microsoft:**



- And with **Safelayer Toolkits** also the SHA-256 chain is validated.

We think this is a bug because the *keyIds* of the *AuthorityKeyIdentifier* of the hierarchy and the final certificate are correct.

Note: we also think the problem is that the hierarchy has UFT-8 codification and the SSL certificate has PrintableString, and maybe the algorithm that uses Firefox for building the certification chain is affected by this.

The certificates we are using for this test can be found at:

http://www.catcert.cat/content/download/6700/16189/file/EV_certificate.zip