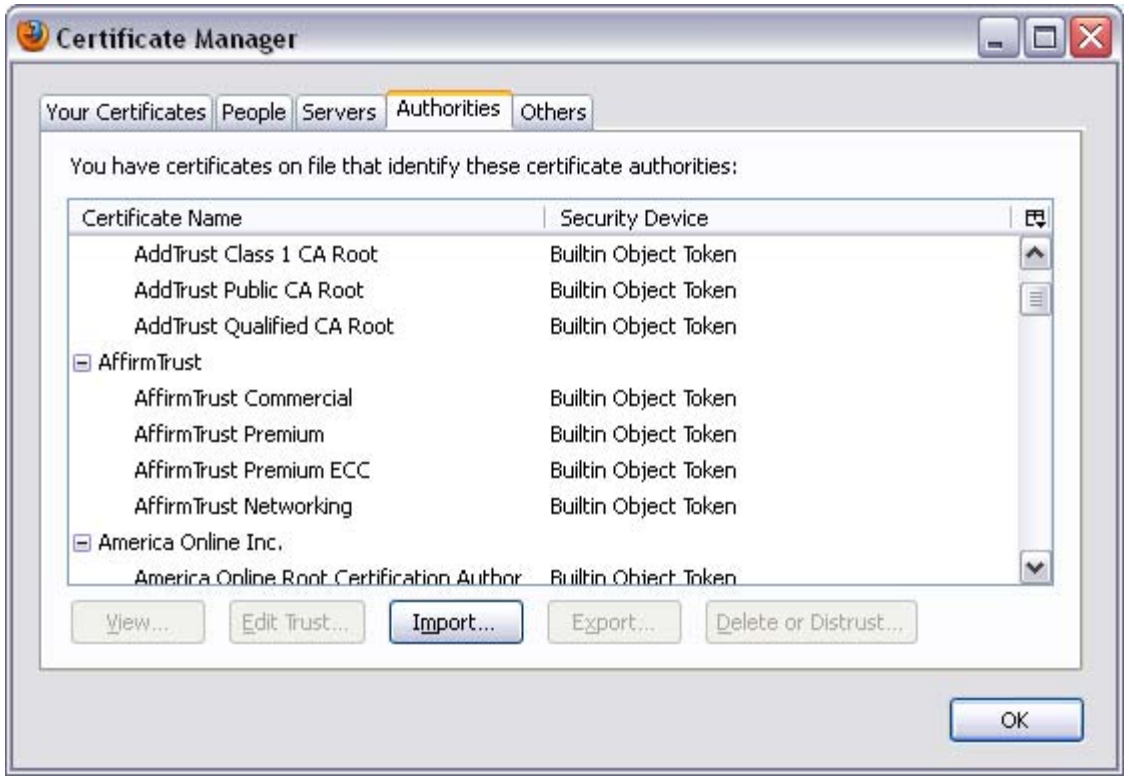
TEST 1 – AFFIRMTRUST'S ROOTS

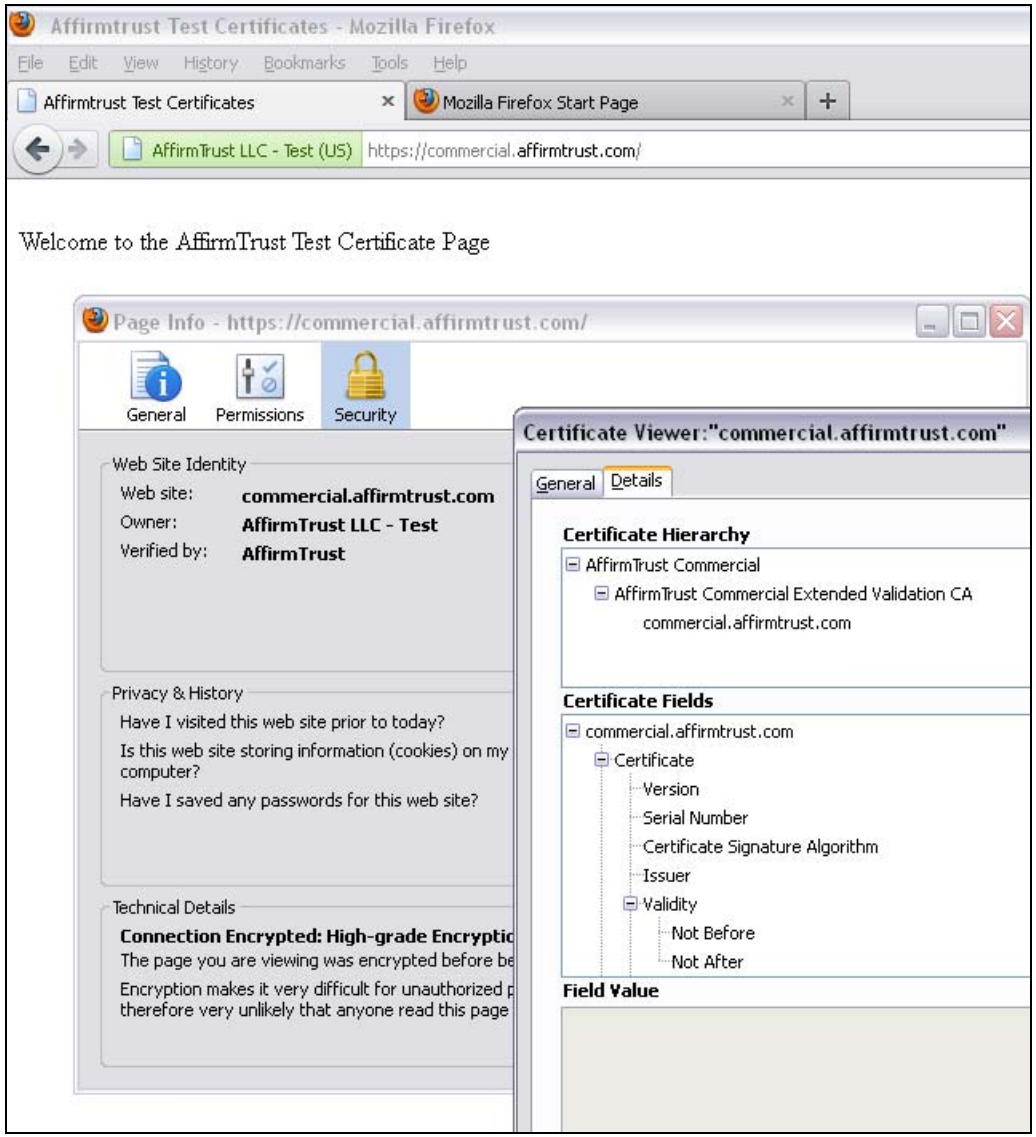
When we have a fresh standard download of FF 6.0 with no preferences, here is the root store. The four AffirmTrust roots are included, but no sub-CAs.



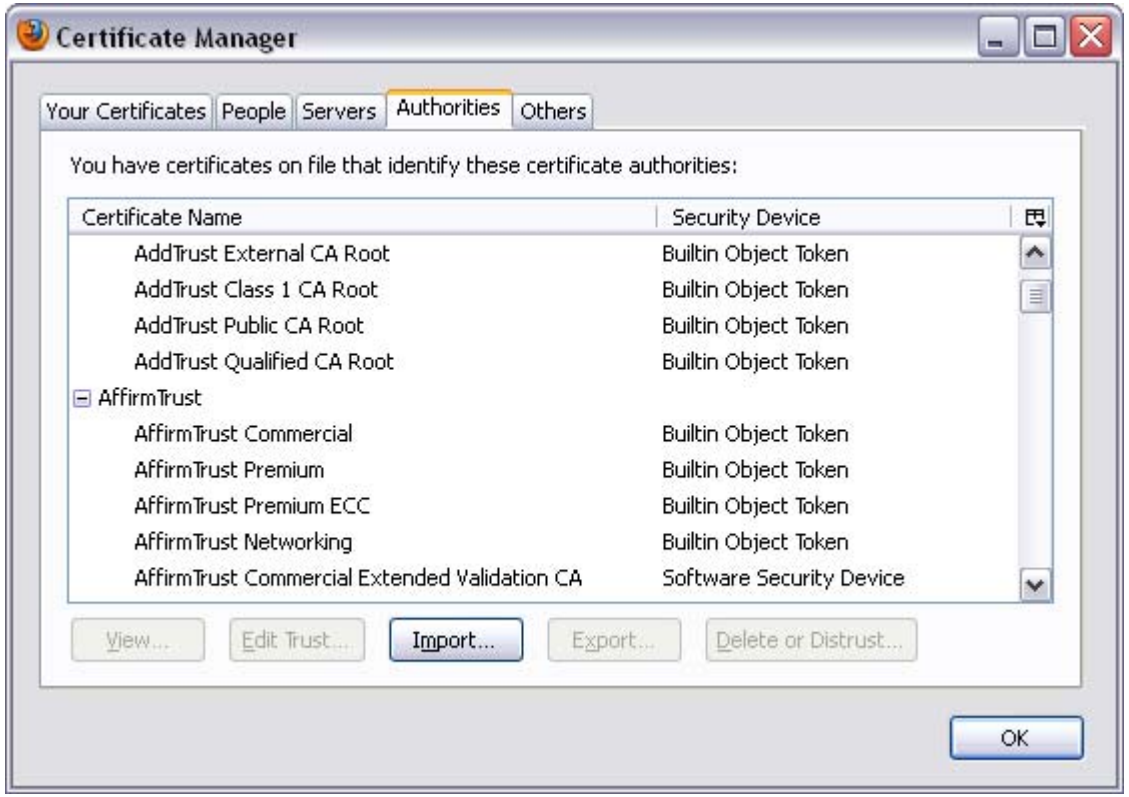
Next we visit any of the four AffirmTrust EV test URLs:

https://commercial.affirmtrust.com/
https://networking.affirmtrust.com:4431/
https://premium.affirmtrust.com:4432/
https://premiumecc.affirmtrust.com:4433/

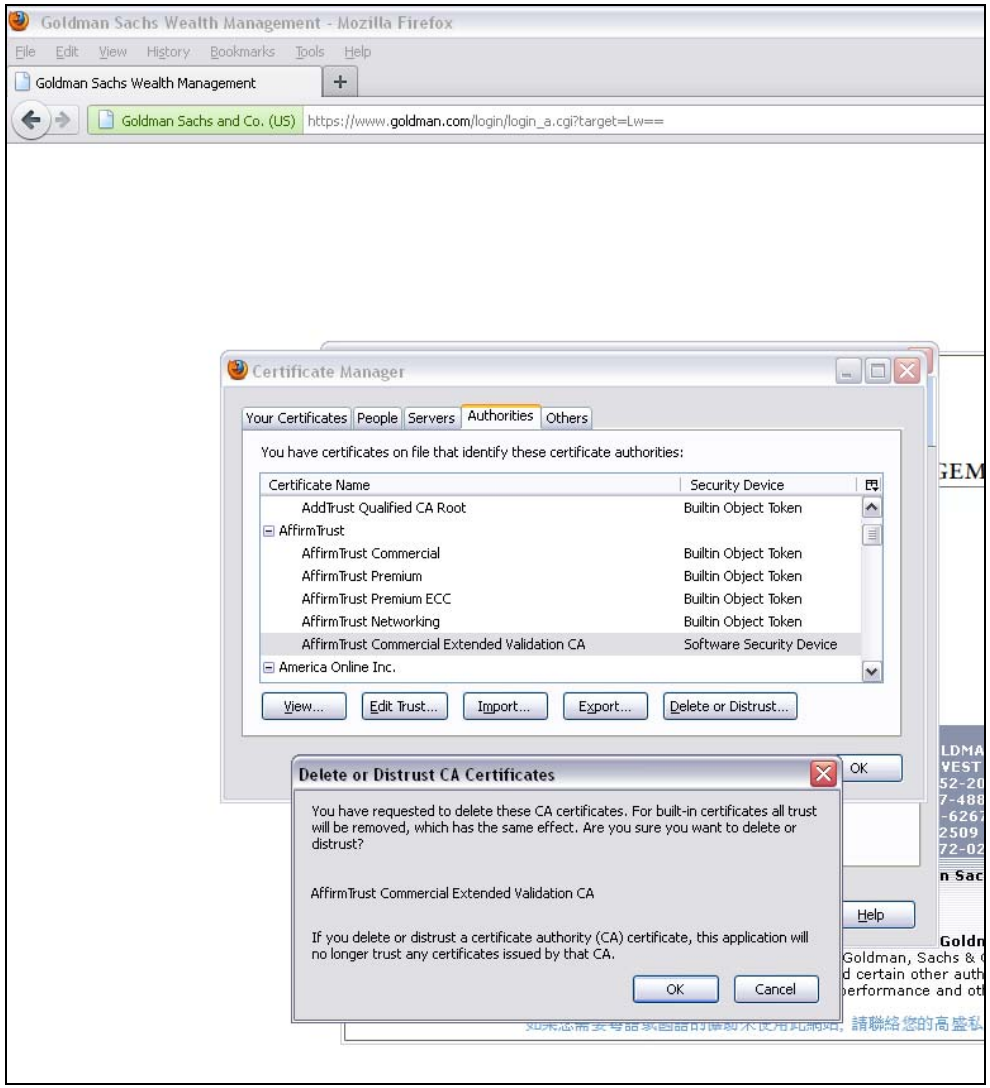
Using the first URL for the Commercial root, we get the green bar:



We also see that the FF 6.0 root store has ADDED the AffirmTrust Commercial Extended Validation CA sub-CA:

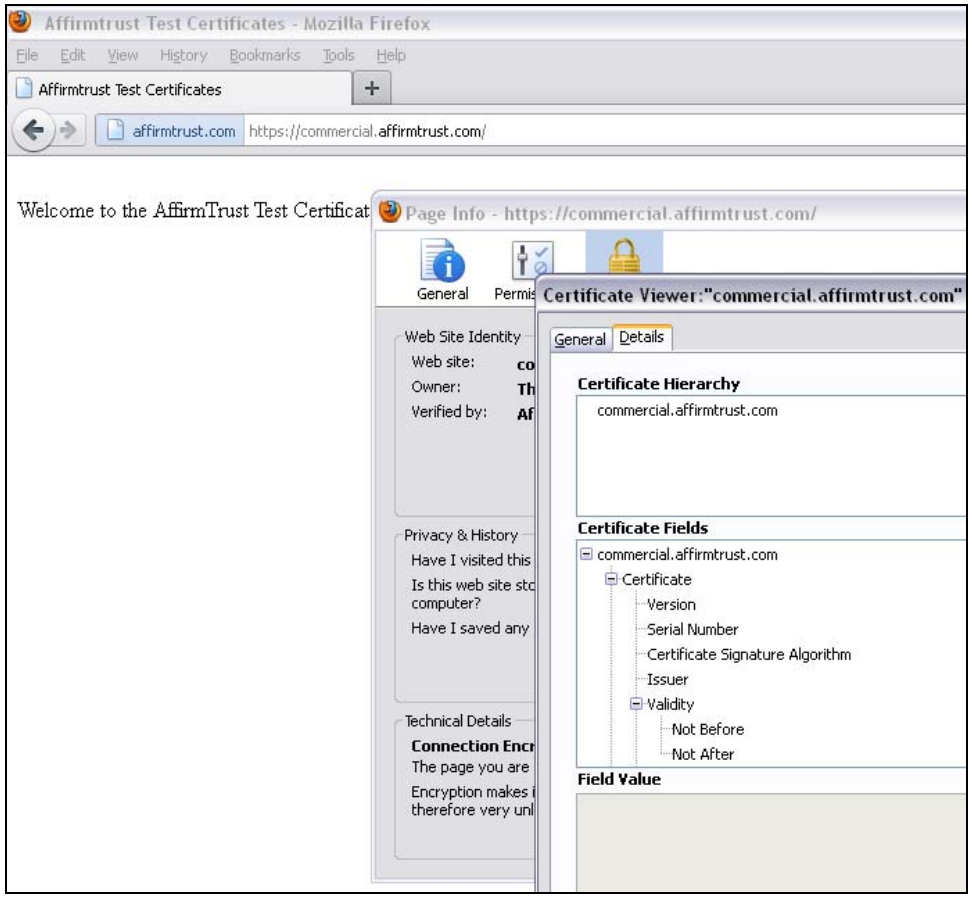


Next, we manually <u>remove</u> the AffirmTrust Commercial Extended Validation CA sub-CA:

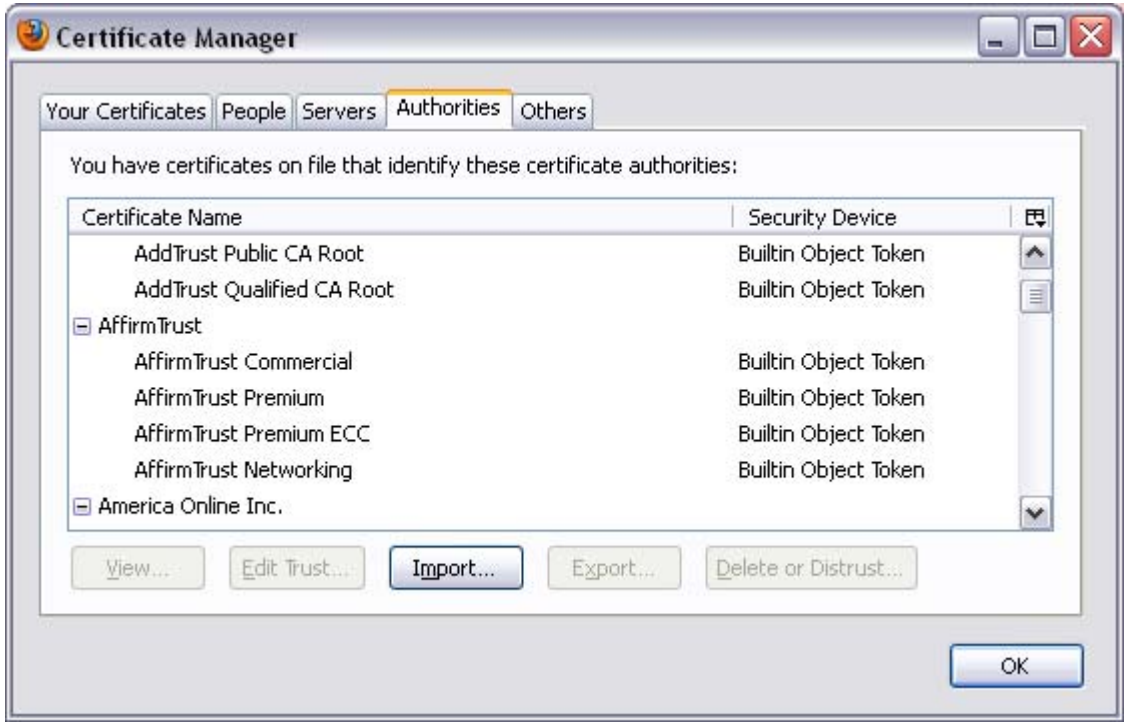


Now, when we return to the same AffirmTrust Commercial EV test URL, https://commercial.affirmtrust.com/, we no longer get the green bar:

Our sub-CA AffirmTrust Commercial Extended Validation CA sub-CA has not been downloaded – and the end-entity certificate securing the test URL does not show ANY hierarchy – not the issuing sub-CA or even the Root! Yet it still gets a blue bar, indicating it comes from a trusted root – but which one? No trusted root is shown:



Likewise, the sub-CA AffirmTrust Commercial Extended Validation CA is not in the root store any more (although the roots remain).



However, the result is very different for VeriSign's roots – see test screen shots on the following pages.

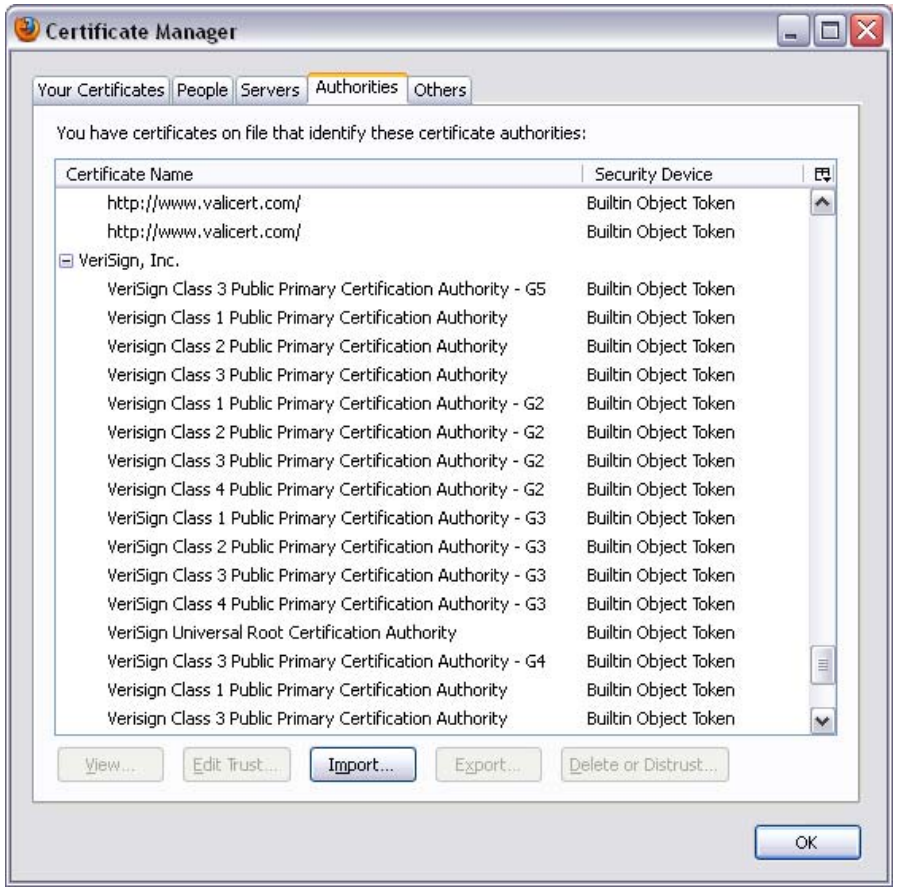
END OF TEST 1

TEST 2: VERISIGN'S ROOTS

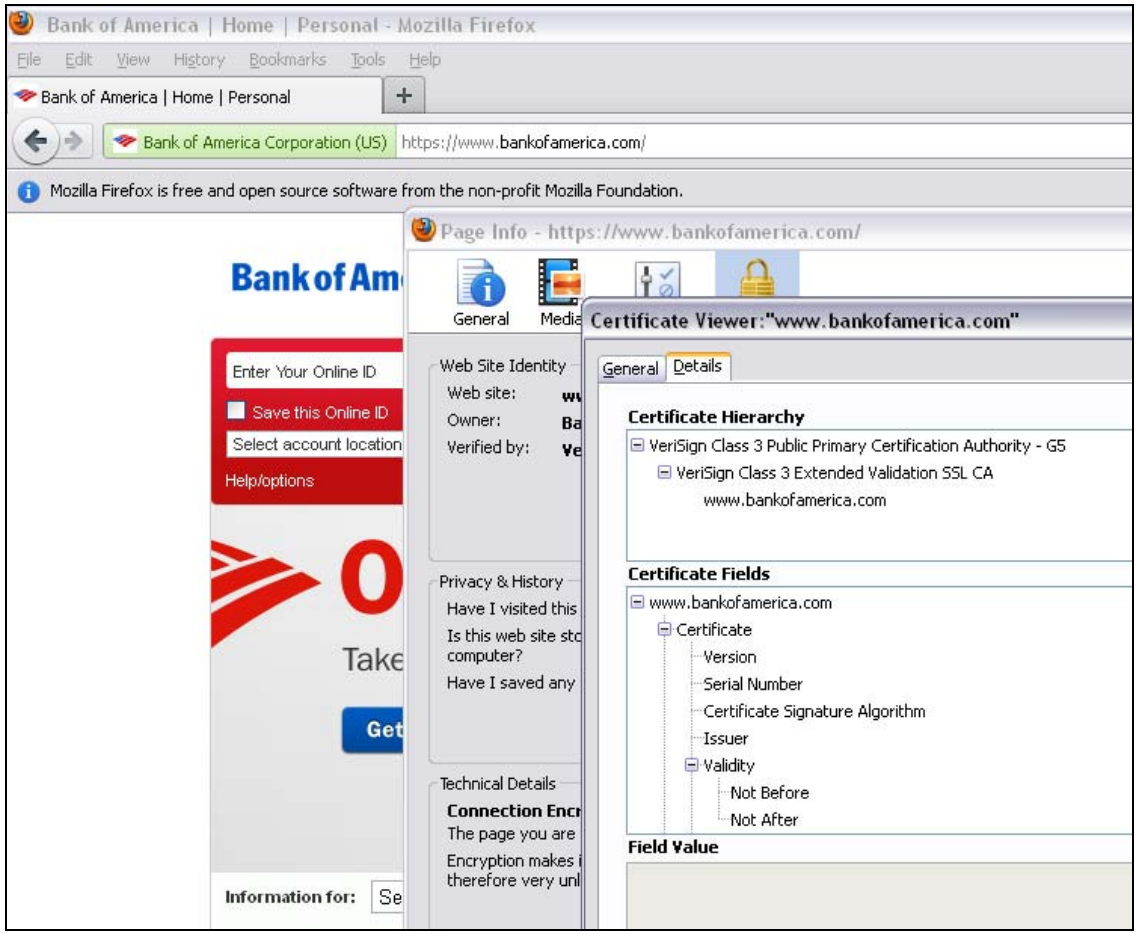
We will conduct the same test for the VeriSign roots at two VeriSign EV sites secured by different VeriSign issuing sub-CAs:

https://www.bankofamerica.com
http://www.goldman.com (which redirects to a secure page)

First, we have a fresh standard download of FF 6.0 with no preferences, and view the root store. Fifteen VeriSign roots are included, but no sub-CAs.



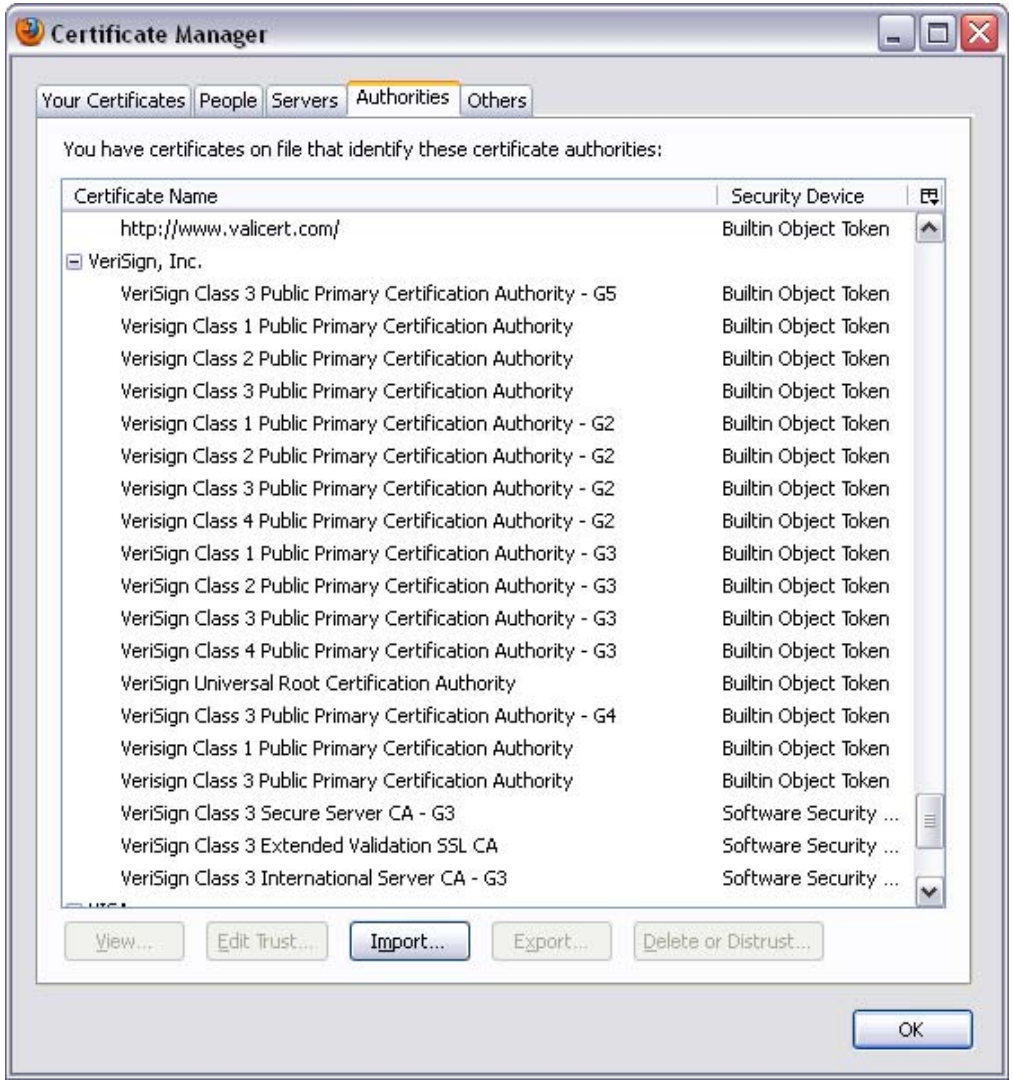
Next, we visit the Bank of America EV site, https://www.bankofamerica.com, and get the green bar. When you view the certificate chain for this site, you see the intermediate issuing sub-CA is named "VeriSign Class 3 Extended Validation SSL CA".



As you see, the site is secured by an EV end-entity certificate issued from the following VeriSign ROOT: **Class 3 Public Primary Certification Authority – G5**, and from the following VeriSign SUB-CA: **VeriSign Class 3 Extended Validation SSL CA**.

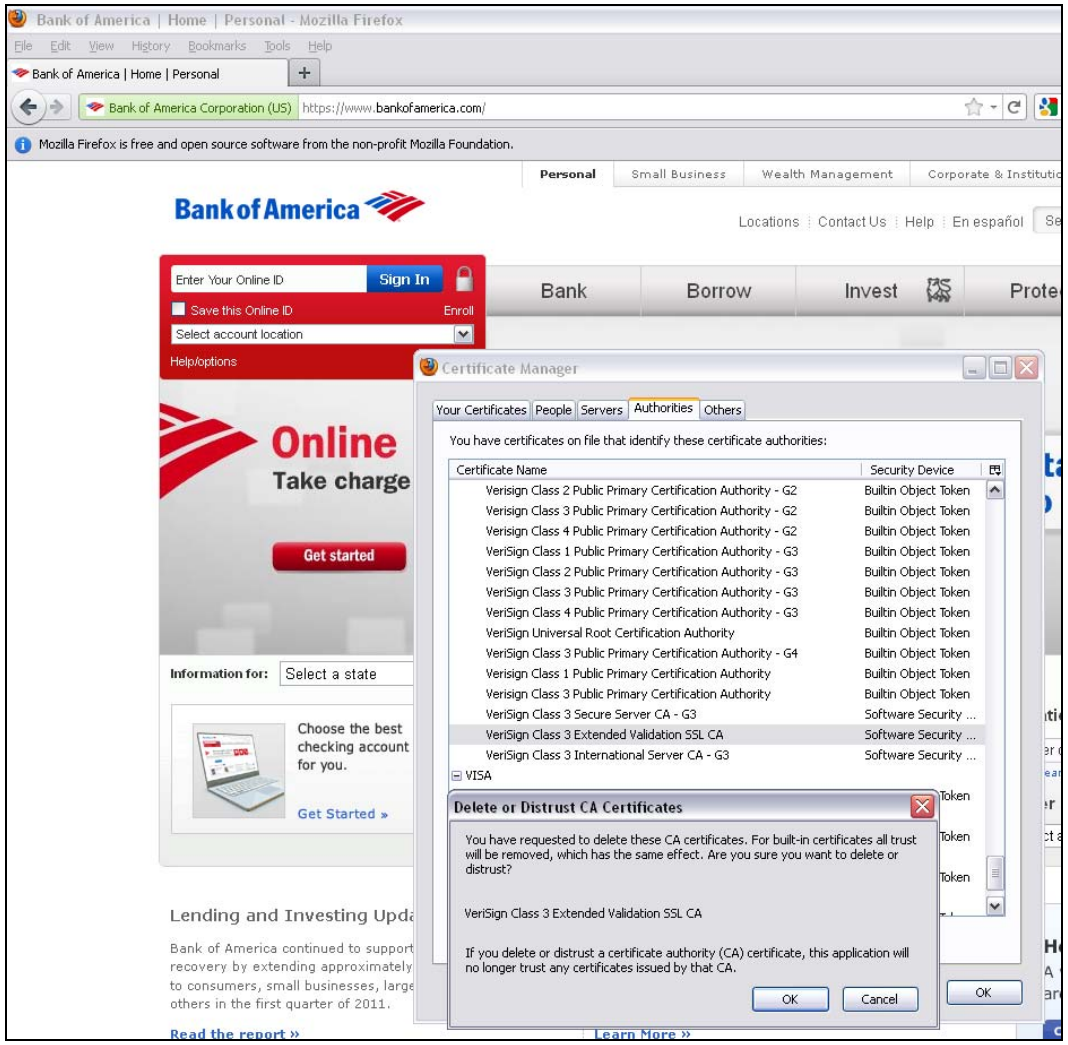
Oddly enough, when we return to the FF 6.0 root store, we now see THREE sub-CAs have been downloaded for VeriSign roots:

VeriSign Class 3 Secure Server CA – G3
VeriSign Class 3 Extended Validation SSL CA [the only sub-CA in the chain securing the Bank of America EV site]
VeriSign Class 3 International Server CA – G3

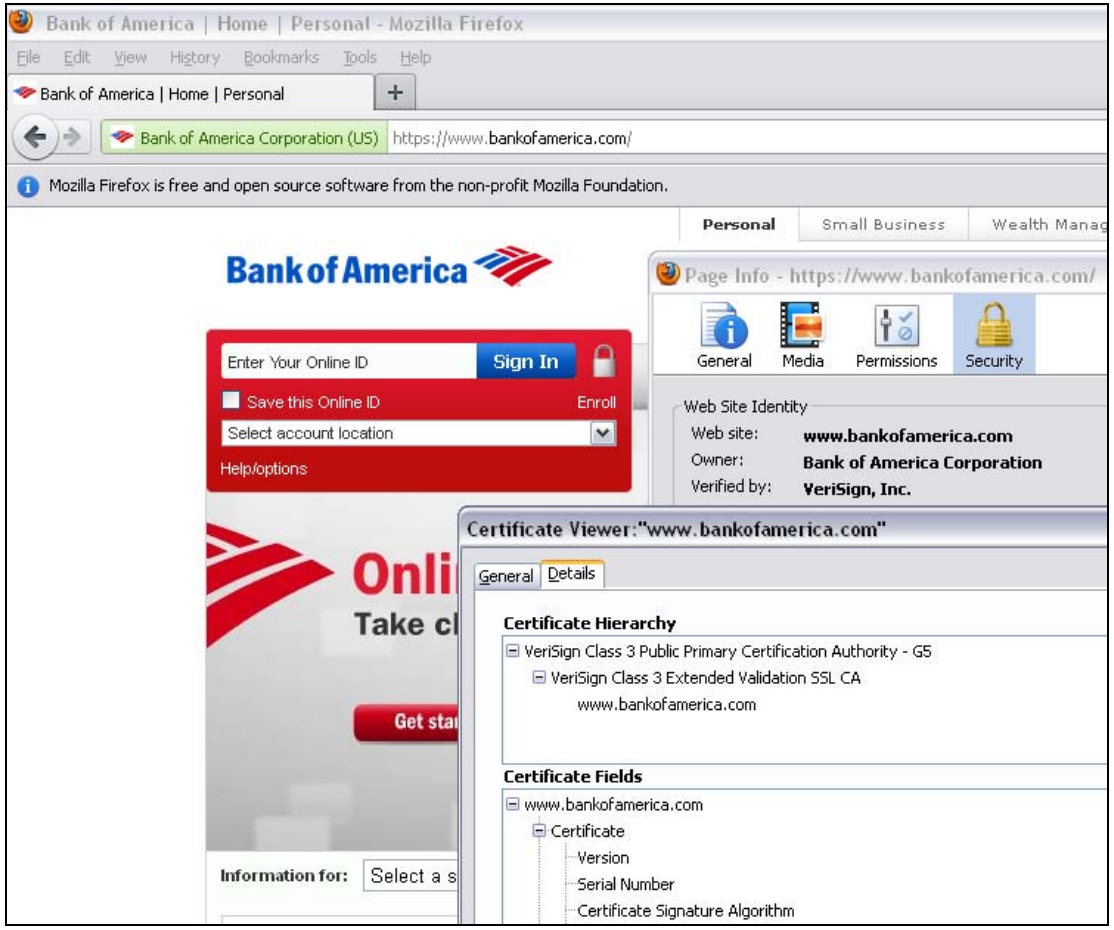


Question: Why did a visit to the Bank of America EV site result in THREE sub-CAs being downloaded to the Mozilla FF 6.0 trusted root store, not just the issuing sub-CA?

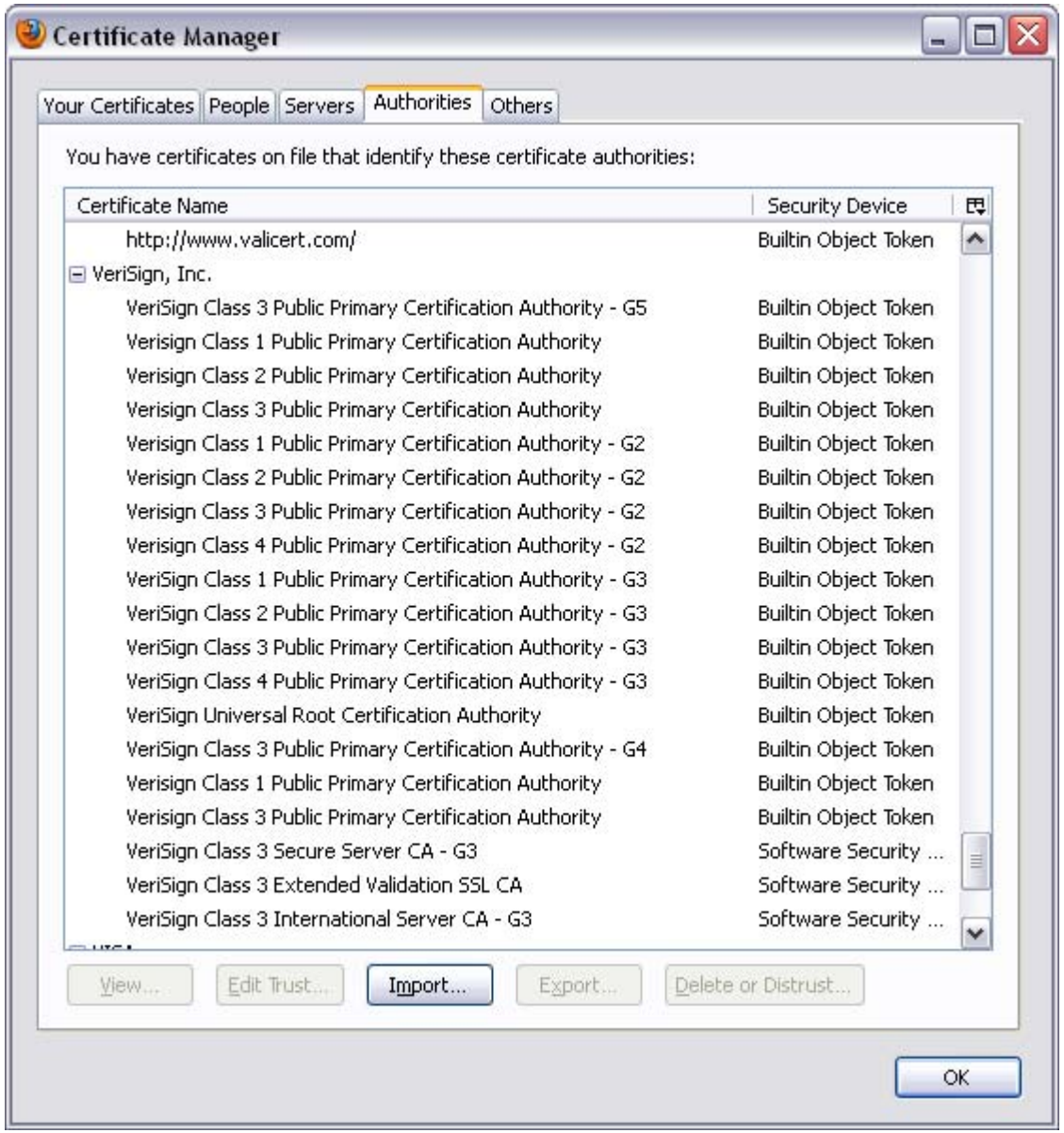
Next, we delete/distrust the issuing sub-CA, **VeriSign Class 3 Extended Validation SSL CA**:



But when we return to the site https://www.bankofamerica.com, we continue to see the green bar, and the issuing sub-CA **VeriSign Class 3 Extended Validation SSL CA** continues to show in the root chain for the site (see below). This is very different for the results with AffirmTrust's roots:



When we return to the FF 6.0 trusted root store, it appears the root store had **again** DOWNLOADED the sub-CA **VeriSign Class 3 Extended Validation SSL CA** even though we previously removed / distrusted the sub-CA:

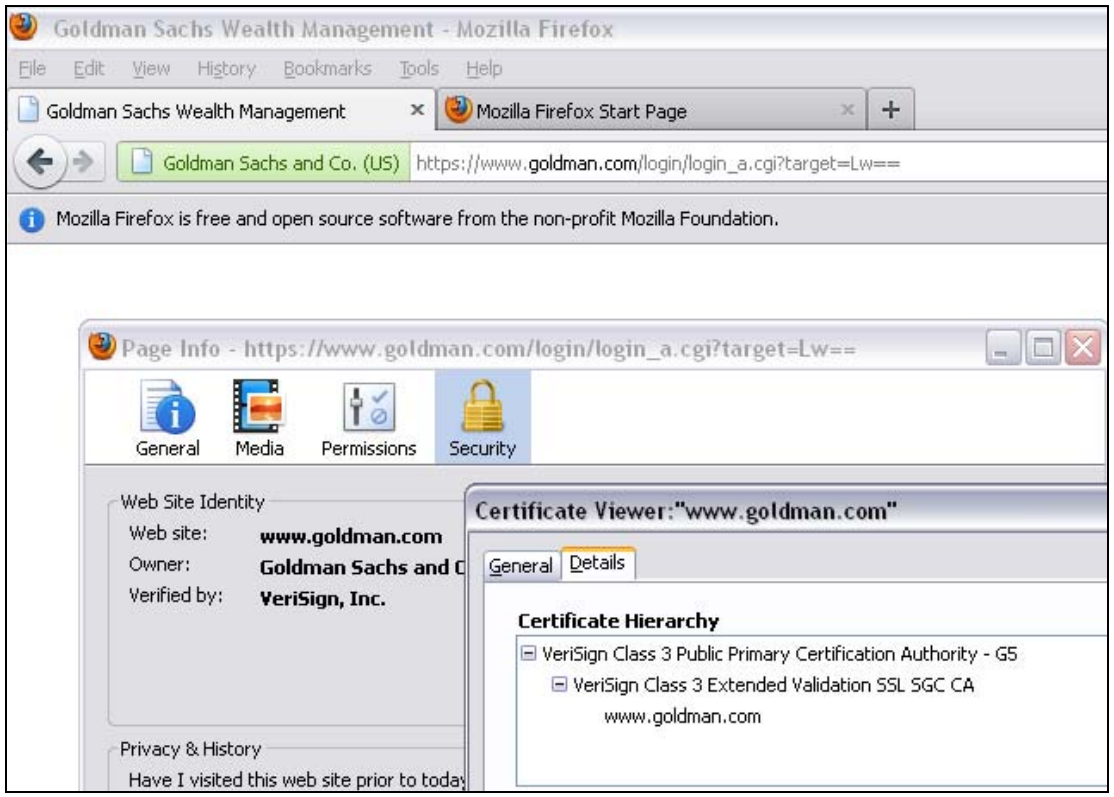


QUESTION: Why did FF 6.0 re-load the issuing sub-CA that was previously removed for the VeriSign root, but did not re-load the issuing sub-CA that was previously removed for the AffirmTrust root?

END OF TEST 2

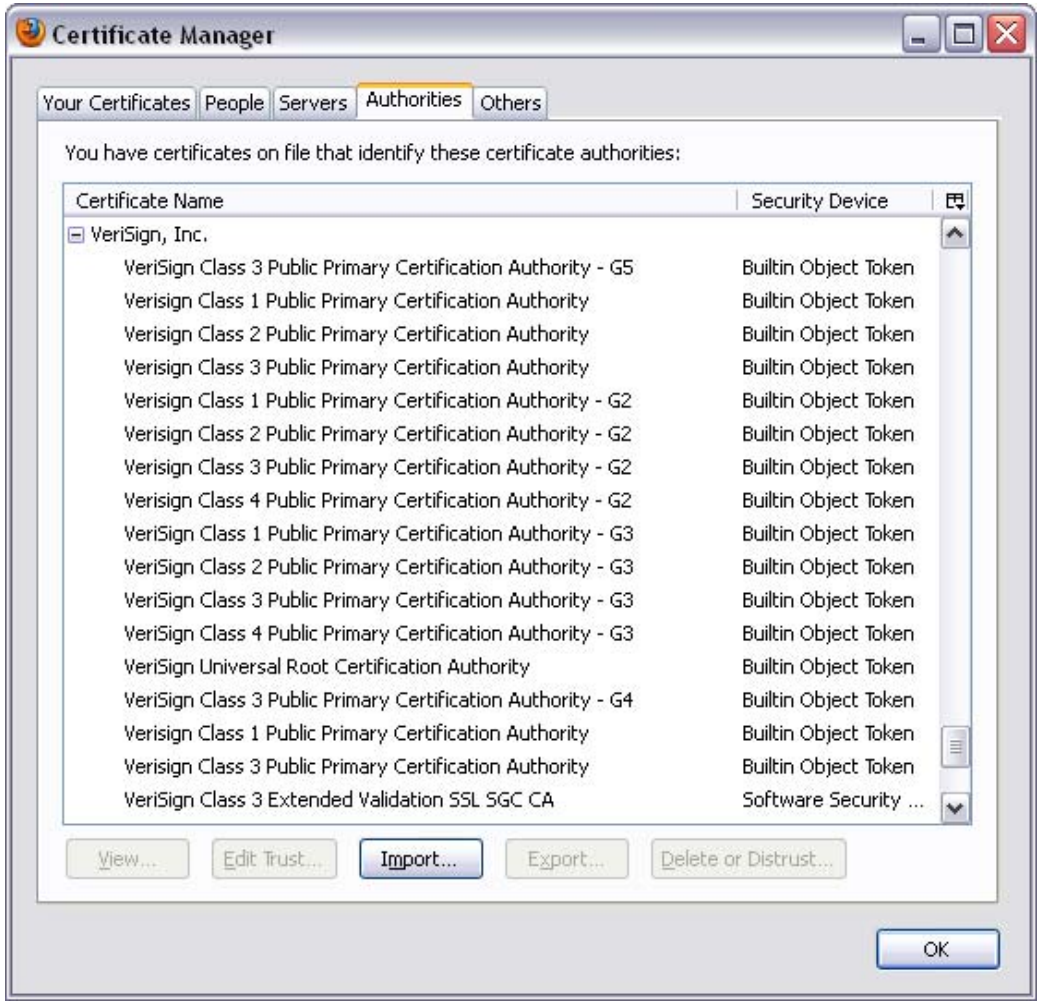
TEST 3: GOLDMAN SACHS EV SITE

A similar result is true when we visit http://www.goldman.com (which then redirects to a VeriSign EV secured page):

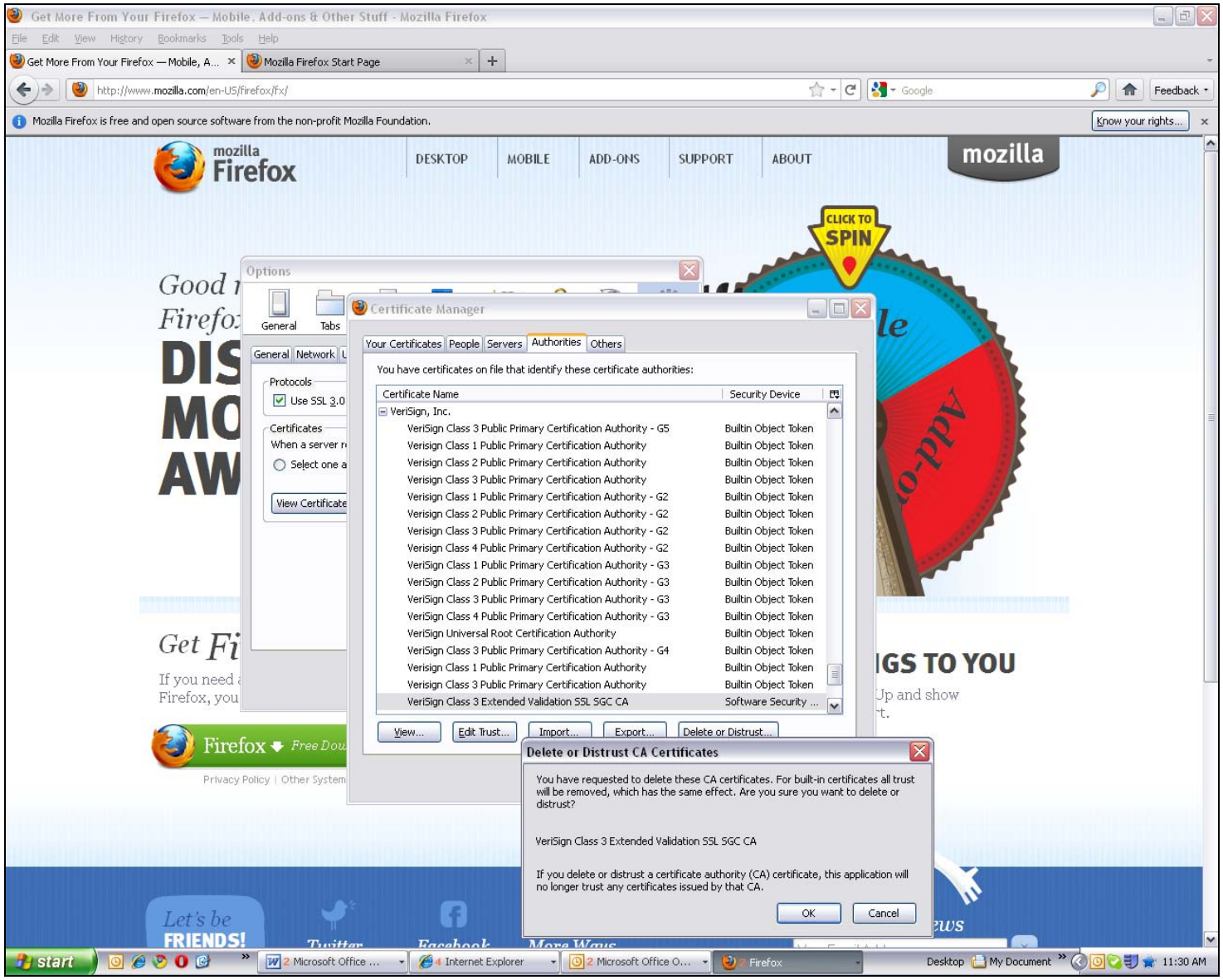


When you visit the Goldman site, you see that it is secured by an EV cert issued from the same VeriSign root as secured the Bank of America EV site, **Class 3 Public Primary Certification Authority – G5**, but the actual EV certificate was issued by a **DIFFERENT** sub-CA than the Bank of America site, the **VeriSign Class 3 Extended Validation SSL SGC CA**.

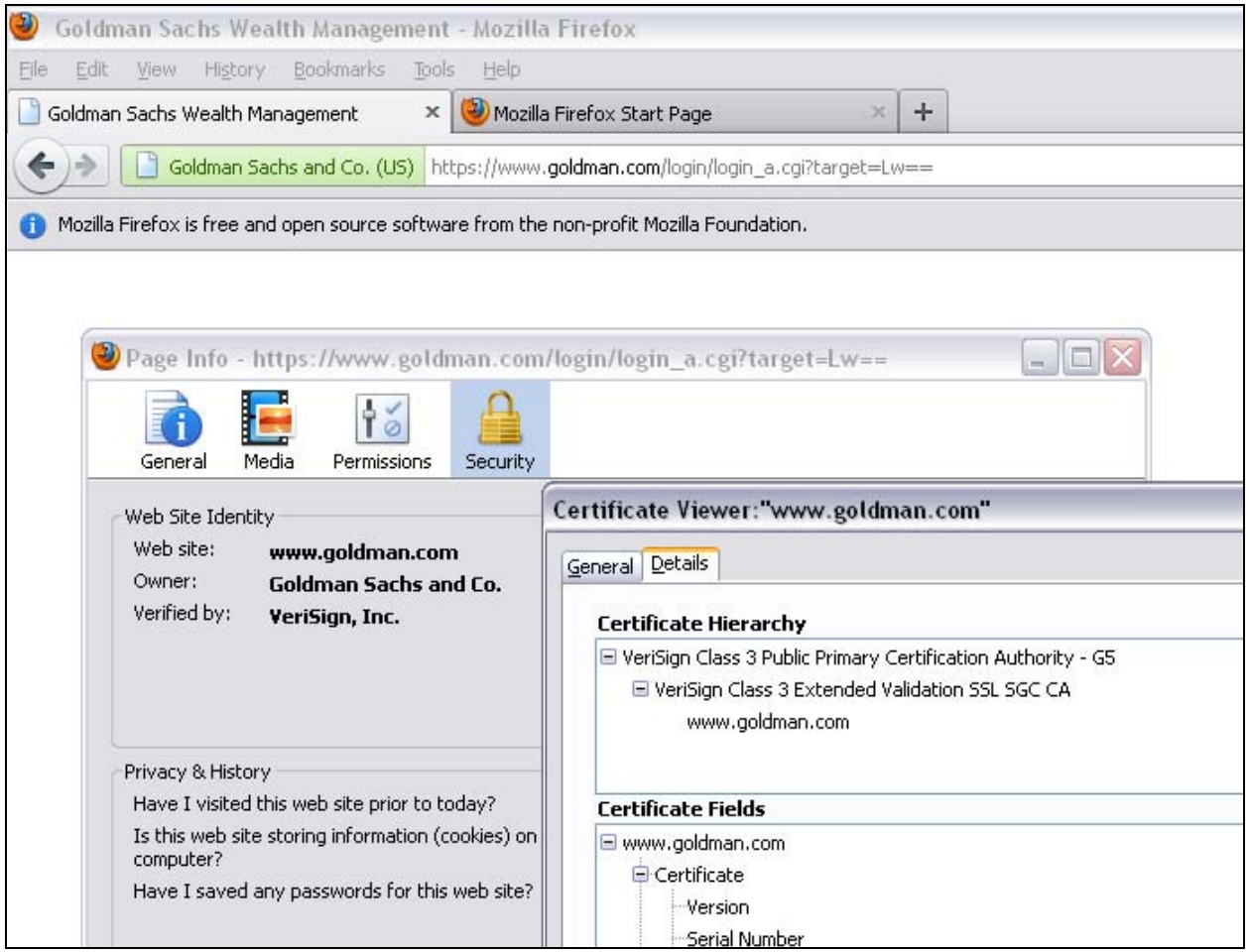
Oddly enough, this time only ONE sub-CA is downloaded when you visit the Goldman site, the issuing sub-CA **VeriSign Class 3 Extended Validation SSL SGC CA** (recall that at the Bank of America EV site, two other sub-CAs were automatically downloaded to the FF 6.0 root store along with the issuing sub-CA):



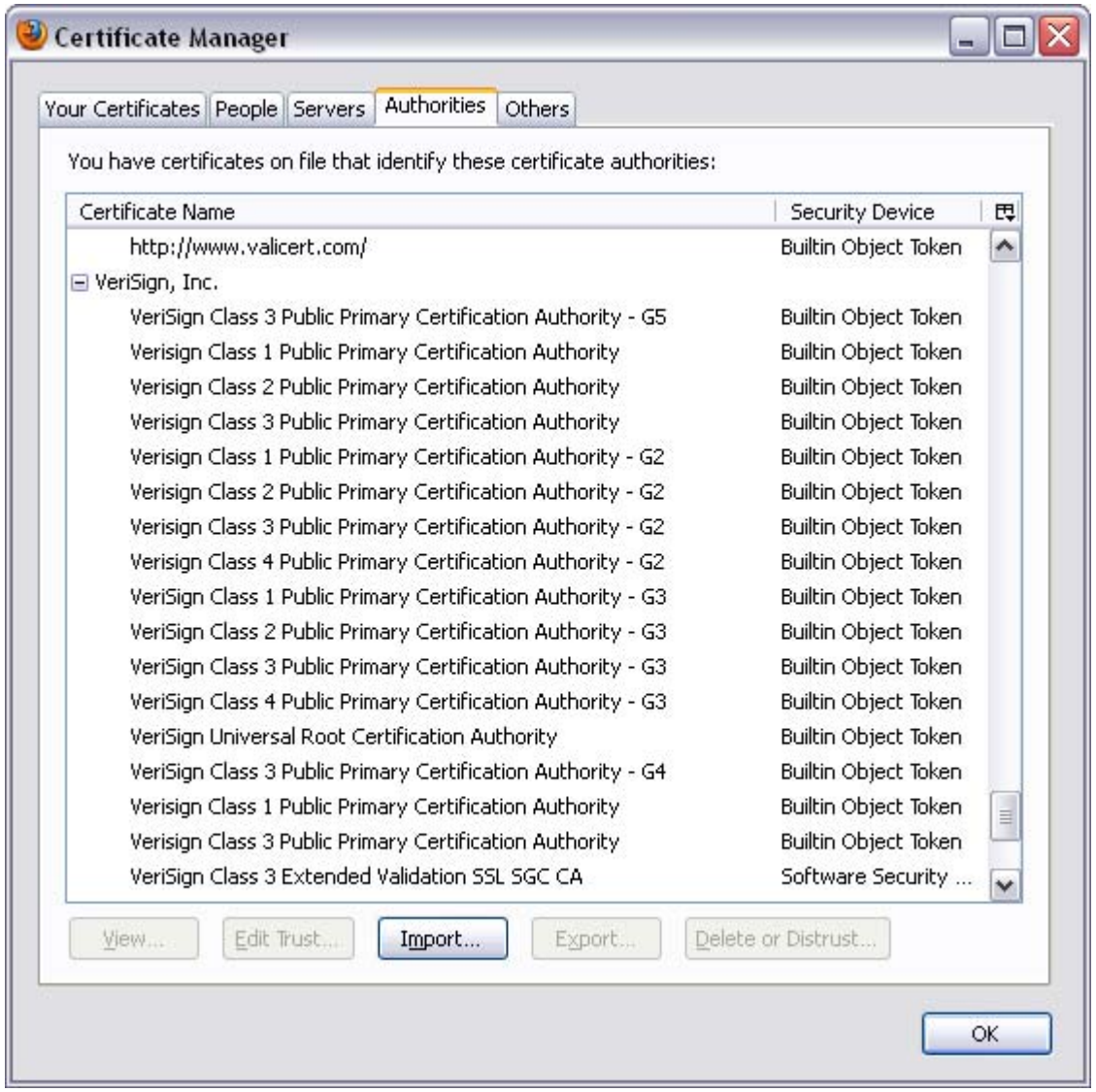
Next, we manually remove / distrust this sub-CA, **VeriSign Class 3 Extended Validation SSL SGC CA.**



When we return to the site http://www.goldman.com, once again the green bar shows, and once again FF 6.0 has DOWNLOADED the issuing sub-CA, **VeriSign Class 3 Extended Validation SSL SGC CA**, even though we just manually removed / distrusted the issuing CA.



When we return to the root store, the issuing sub-CA shows AGAIN, even though we previously removed / distrusted it:



END OF TEST 3

<u>SUMMARY</u>: Again, why does FF 6.0 keep downloading and restoring the VeriSign issuing sub-CAs correctly every time you visit a VeriSign secured EV site (and in some cases, FF 6.0 downloads three VeriSign sub-CAs, not just the issuing sub-CA) even after the sub-CAs have been manually removed / distrusted, but <u>NOT</u> for the AffirmTrust secured EV sites?