

The Opera Rootstore

The Roots of Internet trust

[Blog](#) | [Archivo](#) | [Acerca de](#)



Secom, CNNIC, Buypass Root, Izenpe EV-enabled, and more

BY [YNGVE NYSÆTER PETERSEN](#) WEDNESDAY, 30. SEPTEMBER 2009, 13:39:26

[TLS](#), [UPDATE](#), [SSL](#), [REPOSITORY](#), [CRL](#), [EXTENDED VALIDATION](#), [ROOT CERTIFICATES](#), [OCSP](#), [OPERA BROWSER](#)

We have now added the following Roots to the repository:

- [Buypass](#), a Norwegian CA. This CA has been provisionally EV enabled, please see below. Testsites [1](#), [2](#), [EV](#).
- [CNNIC](#), China Internet Network Information Centre. [Testsite](#). Note: Currently we are missing a HTTP CRL for the intermediate certificate for this site, so the site will unfortunately not show a padlock. We are working with CNNIC to resolve the problem, which may include adding a [CRL override](#).
- [Secom](#) (a Japanese CA) has issue a new SHA-256 Root, as part of many CAs transition to more secure certificate signatures: [Testsite](#)

We have also restored the "Verisign International Server CA" intermediate CA certificate, and updated to the most recent version of the certificate, which is valid to 2016. This is a certificate that Opera shipped with until Opera 7.2x in 2004, when that version of the certificate expired, though newer versions of the certificate have been issued and used by servers.

Recently however, the old expired certificate started to cause problems. The old certificate is still present in many Opera profiles which has been updated continuously from Opera 7.x or before, and therefore caused certificate verification problems (even for the Opera CEO). We did work around it when problems occurred in the Opera 10.00 beta after we changed the certificate verification procedure in order to update the [Verisign G1 Roots to SHA-1](#).

Even more recently other problems started to appear (though they may have been there for a while), and we discovered that a number of mis-configured sites are still using the old expired certificate. This triggered certificate warnings in all versions of Opera before Opera 10.00. In Opera 10.00 these sites triggered a more severe error message, since the expired certificate is signed with the now insecure MD2 method. This is no longer supported in Opera 10.00, and therefore triggers a certificate signature verification failure which is code "554".

These problems should be fixed at server side by installing the newest certificate. The number of sites with the problem that came to our attention indicates that there are too many sites for us or Verisign to play Whack-a-mole that way. After speaking with Verisign about it, we decided to reintroduce the certificate and now require it in all installations. This certificate will therefore be automatically downloaded to Opera the next time it does its weekly check of the repository, replace existing older installed versions of the certificate, and override the certificates used by web sites.

Additionally a couple of bugs in the backend producing the files on the server have been fixed. These bugs may have caused some problems during the past several months.

We have also noticed a problem with [DigiNotar's](#) OCSP responder, and have temporarily added an [OCSP override](#) while working with DigiNotar to resolve the problem.

EV enabled CAs:

- [Izenpe](#), a Basque CA [added](#) in 2008, was EV enabled a few weeks ago, but the announcement was delayed due to the more [significant problem](#) we fixed at the time. [Testsite](#)
- [Buypass](#) is provisionally EV enabled based on their EV Readiness audit ([testsite](#)); the full audit is expected by the end of the year. Please note that at the moment Buypass EV will only be indicated in Opera 10.00 and later. The reason is that Buypass is not using intermediate CA certificates to issue EV certificates (nothing wrong with it, but it is the first CA we have seen to do so). This triggered a

logical problem with the EV check in Opera 9.50 to 9.64 which has been fixed in Opera 10.00. If Buypass starts issuing EV certificates from intermediate CA certificates, those certificates will also show as EV in Opera 9.50 and later.

- Several more [Comodo](#) Roots have been EV-enabled. These certificates should have been EV enabled a year ago, but due to an error on our side they were not. We apologize to Comodo for this error. Testsites: [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7](#), [8](#), [9](#), [10](#), [11](#), [12](#)
- The EV enabled status of several CAs has been extended after we received their updated audits.



yngve



japan-desktop



WildWildPanter



Chas4



illify

As usual, these updates become active and available after the weekly check for updates, but that update can be forced by going to the Opera Toolbar: Help -> Check for updates. The exception is Opera 10.00 where a [bug](#) which is fixed in Opera 10.10, and will be fixed in Opera 10.01, disabled the certificate repository updates. A workaround for the problem in Opera 10.00 is to 1) Shut down Opera, 2) delete/rename the file "tasks.xml" in the profile folder, 3) Restart Opera.

Share this

◊ [Temporarily missing EV indication with Verisign EV certificates](#)

Escribir un comentario

Debes entrar para escribir un comentario. Si no eres miembro activo [regístrate](#).

Usuario:

Contraseña:

Try a faster and more secure Web browser. [Descárgate Opera](#)



The Opera Rootstore is blogging on My Opera

My Opera is a blog and photo sharing community with millions of members.

[Join now](#) to follow The Opera Rootstore's blog and get your own.

[Join now!](#)

[Ayuda](#) | [Descargo de responsabilidad](#) | [Términos y condiciones](#) | [Web analytics powered by HitsLink](#)

[RSS](#) | [ATOM](#) | [WIDGETIZE](#)

Site language: [Español](#)