DST Root CA X3 Expiration (September 2021)

Last updated: May 7, 2021 | See all Documentation

On September 30 2021, there will be a small change in how older browsers and devices trust Let's Encrypt certificates. If you run a typical website, you won't notice a difference - the vast majority of your visitors will still accept your Let's Encrypt certificate. If you provide an API or have to support IoT devices, you might have to pay a little more attention to the change.

Let's Encrypt has a "root certificate" called ISRG Root X1. Modern browsers and devices trust the Let's Encrypt certificate installed on your website because they include ISRG Root X1 in their list of root certificates. To make sure the certificates we issue are trusted on older devices, we also have a "cross-signature" from an older root certificate: DST Root CA X3.

When we got started, that older root certificate (DST Root CA X3) helped us get off the ground and be trusted by almost every device immediately. The newer root certificate (ISRG Root X1) is now widely trusted too - but some older devices won't ever trust it because they don't get software updates (for example, an iPhone 4 or an HTC Dream). Click here for a list of which platforms trust ISRG Root X1.

DST Root CA X3 will expire on September 30, 2021. That means those older devices that don't trust ISRG Root X1 will start getting certificate warnings when visiting sites that use

Let's Encrypt certificates. There's one important exception: older Android devices that don't trust ISRG Root X1 will continue to work with Let's Encrypt, thanks to a special cross-sign from DST Root CA X3 that extends past that root's expiration. This exception only works for Android.

What should you do? For most people, nothing at all! We've set up our certificate issuance so your web site will do the right thing in most cases, favoring broad compatibility. If you provide an API or have to support IoT devices, you'll need to make sure of two things: (1) all clients of your API must trust ISRG Root X1 (not just DST Root CA X3), and (2) if clients of your API are using OpenSSL, they must use version 1.1.0 or later. In OpenSSL 1.0.x, a quirk in certificate verification means that even clients that trust ISRG Root X1 will fail when presented with the Android-compatible certificate chain we are recommending by default.

If you want additional information about our ongoing production chain changes, please check out this thread in our community.

If you have any questions about the upcoming expiration, please post to this thread on our forum.

Let's Encrypt is a free, automated, and open certificate authority brought to you by the nonprofit Internet Security Research Group (ISRG).

548 Market St, PMB 57274, San Francisco, CA 94104-5401, USA

Send all mail or inquiries to:

PO Box 18666, Minneapolis, MN 55418-0666, USA