It's Time to Act If You Have Digital Certificates with Entrust

What's happened?

Google® recently announced that it will no longer trust sites with Entrust digital certificates after October 31, 2024—so, any sites with an Entrust certificate issued after that date will be blocked and labeled "distrusted" when a user tries to access it via the Chrome™ browser.

What do you need to do?

Brands that currently use Entrust digital certificates need a different certificate provider to issue their digital certificates to ensure their sites are still visible to Chrome users.

Key considerations

Pick a vendor that can meet your needs.

You should choose a certificate vendor that puts security first to avoid any future situations like this. CSC is a security-first, enterprise-class provider of domain security solutions that can provide you with:

- Advanced domain security features, including certificates with enhanced validation levels (OV and EV).
- The option to add certification authority authorization (CAA) records to domains in your portfolio for an extra layer of security.
- Automation options to ensure that digital certificates don't lapse, keeping your sites encrypted with no gaps in service.

Make sure they're NIS2 compliant.

For organizations in Europe, or ones doing business with them, being Network and Information Security (NIS2) compliant will be essential. Make sure you evaluate your digital certificate vendor by conducting a risk assessment. Use a questionnaire, including inquiries about security governance, to confirm conformance with NIS2.

Futureproof!

Distrust of Entrust certificates is not the only big change happening in the digital certificate realm. 90-day digital certificate lifetimes are coming. Here's our handy checklist to see if automation is the right solution for your brand:

- Take an inventory of all your publicly trusted certificates.
- Take an inventory of all servers these are installed on, noting the server software (Microsoft®, Apache, Linux, etc.) and the version being run. Verify if these server versions are supported by ACME.
- If all are supported, then automation will be possible.
- If they are NOT supported, check out our **SSL Automation** web page to see your options.

CSC offers multiple solutions from public key infrastructure (PKI) to application programming interface (API) implementations tailored to your specific use cases.

We're ready to talk.

CSC can meet your domain security needs. If you want to be contacted about switching your digital certificates to CSC, complete our form and one of our experts will contact you.

Get in touch
cscdbs.com