The Slow Death of EV Certificates

In this lesson, we'll learn what EV certificates are and why they aren't necessary.

We'll cover the following

Introduction

More than once in my career I've been asked to provision an EV certificate for web applications, and every single time I managed to get out of it, not because of laziness, but because of the security implications of these certificates. In short, they don't have any influence on security and cost a lot of money. Let's learn what EV certificates are and why you don't need to use one.

What are Extended Validation certificates?

Extended Validation certificates (EV) are a type of SSL certificate that aim to increase the users' security by performing additional verification before the issuance of the certificate. This additional level of scrutiny should, on paper, allow CAs to prevent bad actors from obtaining SSL certificates to be used for malicious purposes, a truly remarkable feat if it worked that way. There were some egregious cases instead, like the one where a researcher named Ian Carrol was able to obtain an EV certificate for an entity named "Stripe, inc" from a CA. Long story short, CAs are not able to guarantee an increased level of security for EV certificates.

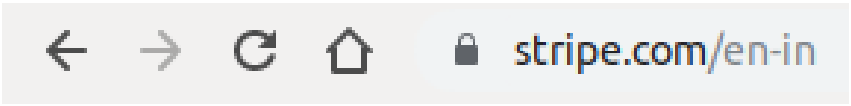
They made for pretty UI

If you're wondering why EV certificates are still used, let me give you a quick answer, under the false assumption of added security, EV certificates used to have a special UI in browsers, sort of a vanity feature CAs would charge an exorbitant

amount of money for (in some cases more than $1,000 for a single-domain EV certificate). This is how an EV certificate would show up in the user's browser:

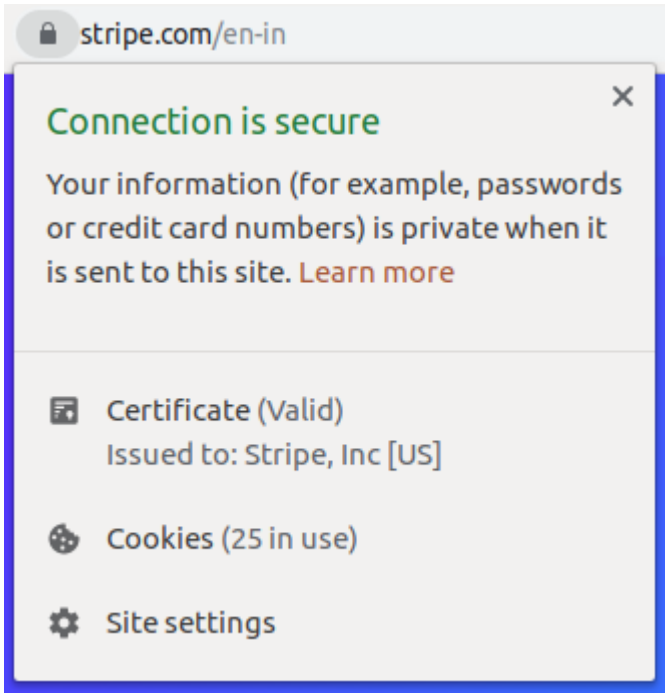
EV certificates made for pretty UI

As you can see, there is a nice UI pattern here, but the problem is it's of no use from a security perspective. As soon as research started to point out how ineffective EV certificates are in terms of security, browsers started to adapt, discouraging websites from purchasing EV certificates. This is how the browser bar looks like when you access stripe.com from Chrome 77 onwards.



The UI for EV certificates was degraded when their ineffectiveness was demonstrated

The additional information (such as the organization's name) has been moved to the "Page Info" section, which is accessible by clicking on the lock icon on the address bar.



Additional information shown by clicking on the lock icon

They really are dead

Mozilla has implemented a similar pattern starting with Firefox 70; so it's safe to say, you shouldn't bother with EV certificates anymore:

- They do not offer any increased level of security for your users
- They do not get a preferential UI at the browser-level, making it a very inefficient expense compared to regular SSL certificates you can obtain (Let's Encrypt certificates are free, for example)

Troy Hunt summed the EV experience quite well:

> *EV is now really, really dead. The claims that were made about it have been thoroughly debunked and the entire premise on which it was sold is about to disappear. So, what does it mean for people who paid good money for EV certs that now won't look any different to DV? I know precisely what I'd do if I was sold something that didn't perform as advertised and became indistinguishable from free alternatives...*
>
> **Troy Hunt - Extended Validation Certificates are (Really, Really) Dead**

In the next lesson, we'll learn that it's better to be paranoid than to risk an attack.