



What is Let's Encrypt?

Why Let's Encrypt isn't ideal for businesses

Let's Encrypt (LE) is a non-profit Certificate Authority (CA) that issues free 90-day Domain Validated SSL certificates. This is a phenomenal service for small websites and blogs **where the owner has no financial stake** and is just looking to **add no-frills encryption**. But while Let's Encrypt is a good service with noble intentions, **it's a poor choice** for any company or organization that does business online.



The benefits of going with a traditional CA over Let's Encrypt

Traditional CA



- ✓ Offers Organization Validation (OV) & Extended Validation (EV) SSL Certificates
- ✓ Invests in **security infrastructure** to help prevent issuing to cybercriminals
- ✓ 1-2 year certificate lifespans available
- ✓ Customer service is readily available in multiple languages **24/7/365**
- ✓ In the event of a **vulnerability**, the CA can mass-revoke affected certificates

Let's Encrypt



- ✗ Offers only **Domain Validation (DV)** SSL, which provides minimal authentication
- ✗ **Minimal safeguards**, issues certificates without even performing email validation
- ✗ All certificates have 90-day lifespans
- ✗ Community-based support model – **customers self-diagnose and troubleshoot**
- ✗ In the event of a vulnerability, Let's Encrypt has **no mechanism to mass-revoke**

Businesses Need Higher Assurance



Phishing attacks are on the rise



People are learning DV ≠ safe



OV/EV offers greater assurance of ID



A Trusted CA authenticates your company



The certificate displays verified info



Site Seals boost trust and conversions

Trust is Key

- ✓ Trust is **vital** to ecommerce
- ✓ Customers **need to know it's you**
- ✓ Business authentication provides **verified proof** of identity
- ✓ Higher assurance = **higher profits**

Let's Encrypt isn't a business-class solution

Issue

Explanation



LACK OF SECURITY MECHANISMS

No response at scale for vulnerabilities

Let's Encrypt **issues to known phishing and malware domains**, doesn't give user notifications about dangerous sites, faces several known bugs and – perhaps most egregiously – **lacks the ability to respond** in scale to vulnerabilities like Heartbleed.



LET'S ENCRYPT ISSUES TO ANYONE

Including hackers and cybercriminals

According to PhishLabs as of Q3 2018, 49% of HTTPS sites were phishing scams. Many of these malicious sites appear secure using Let's Encrypt DV certificates. When asked if the bad guys use Let's Encrypt, Executive Director Josh Aas told Wired: "Yeah."



NO BUSINESS AUTHENTICATION

Domain Validation isn't enough

Now, more than ever, **internet users demand assurance** about the true identity of the sites they do business with. Only business authentication can provide that level of assurance to **potential customers**. Unfortunately, Let's Encrypt doesn't offer that.



NO PKI CAPABILITIES

Management is messy

Let's Encrypt offers **no way to simplify certificate management**, which becomes even more of an issue considering they expire every 90 days. Growing organizations need tools to make things easier, not give them **something else to worry about**.



TOTAL LACK OF CUSTOMER SUPPORT

We hope you have an IT background

Let's Encrypt is **extremely difficult to manually install** and configure and doesn't offer the option of enterprise-grade support. In fact, because of its non-profit status and tight budgets, all Let's Encrypt **support is entirely crowdsourced**.

Let's Encrypt: Not Designed for Business

While Let's Encrypt is a viable option for small websites & blogs that can't afford to invest in security, **it's a poor choice** for companies or organizations. Lack of business authentication, lack of strong security mechanisms and a lack of customer support are all **major issues that should be considered** when choosing between Let's Encrypt and a traditional CA.

Still have some questions?

Email
thqcyberdivision@gmail.com

Website
<https://thqcyberdivision.github.io>

