A fundamental shift in SSL/TLS practices for a healthier security ecosystem

What is it?
A public record of SSL/TLS certificates issued for domains on the internet.

How does it work?
Certificate Authorities (CAs) like Symantec and other entities set up publicly accessible, tamper-proof Certificate Transparency Log Servers.

Who logs certificates in these servers?
Certificate Authorities can log certificates as part of SSL/TLS issuance. In fact, all certificates issued by Symantec are logged automatically. We even offer privacy options that reveal only root domains so any sensitive subdomain data remains hidden.

This way, even certificates issued prior to Certificate Transparency becoming standard practice may appear in the logs. Anyone who runs across an unlogged certificate can log it on a public server.

Who can access the logs?
Anyone, including:
- Domain Owners
- It Managers
- Certificate Checkers
- Security Apps
- Any Web User
- Browsers

What are the benefits of Certificate Transparency?

- Simplify your certificate management. See all certificates under your domains, quickly spot questionable ones (including development certificates, malicious certificates or those bought from the wrong supplier), and take action quickly.

- Protect your brand’s reputation online. Make it harder for hackers to impersonate your brand by creating a convincing fake website.

- Increase trust and confidence across the entire SSL/TLS certificate ecosystem. Good for the internet. Good for your customers. Good for your business.