# Transport Layer Security Report

## Similarities

All investigated websites do not have any glaring security vulnerabilities with the data provided by SSL Labs. When discussing the certificates themselves, each website presents a 3-step certificate chain following the pattern of Host 🡪 Intermediate Certificate 🡪 Root Certificate. Every website listed supports TLS 1.3, which is the most secure and up-to-date version of TLS 1.3 and contains no major vulnerabilities. Finally, all websites achieve a “B” ranking or above, demonstrating at least strong competence when adhering to internet safety standards.

## Differences

However, the differences are more numerous than the similarities. Throughout the seven websites tested, there is a split between using elliptic curve (EC) and RSA encryption for the keys of the certificates. Elliptic curve keys are the more up-to-date standard when it comes to keys. The websites that use reflect websites EC keys are created more recently and haven’t had the uptime of other websites that still use RSA. But that doesn’t mean that RSA isn’t secure either, it just illustrates the longevity of websites like YouTube, Spotify, and Netflix.

Another aspect of the certificate data that represents the longevity of certain websites is how many different versions of TLS the website uses. The TLS configurations also directly influence the grades of websites, as supporting older versions of TLS introduce vulnerabilities only present in those older versions of TLS. As modern operating systems and browsers use TLS 1.3 now, it is only the people using these older operating systems and browsers that are vulnerable.

Balancing the market share of users still using out of date technology and the security risks of that demographic is a complicated process, and these findings illustrate that companies would rather keep the old infrastructure intact than update their websites to TLS 1.3 and TLS 1.2 exclusively.

## Questions

I was still a little confused on how to extract the specific authentication algorithms that these certifications use, as I was lost with the amount of information the “Cipher Suites” section. How can I more easily parse that information to gather which websites used the most secure algorithms?

Are there any root certificate distributors that are less secure or trustworthy than others?

Are the lengths of the validity periods any indication of how secure a website is?