**Headline:** Why should I know what TLS 1.3 is if I own a business?

Whether you own a digital business or not, you cannot ignore the influence and the popularity of the Internet nowadays. And you are most probably aware of the fact that if you have better internet services for introducing your business, you are a winner! And that is where TLS 1.3 has got something to offer.

TLS 1.3 (Transportation Layer Security) is the latest version of a data transportation security protocol which has the duty of securing the data your client works with through your website. Today, privacy is one of the things that all people worry about and care about indescribably. If you have got a website to introduce your work to the internet or if you haven’t gotten one yet, TLS 1.3 is one way to make sure not only you gain the trust of your clients, but also you gain more of them using your services or products; because they are assured that you value their privacy.

In comparison to its predecessor TLS 1.2, lesser latency (faster connection) while establishing a fully secure connection is what TLS 1.3 guarantees. As a data transportation security protocol, it is highly important to make sure that your data is impossible to be tracked. TLS 1.3 is immune to all types of attacks & vulnerabilities which could be dangerous to your data privacy. TLS 1.3 is also known as a hybrid cryptosystem which means it uses two kinds of cryptography to make sure you have no worries about being far away from attacks of any sort. You might ask how does a hybrid cryptosystem does its work exactly? Since you want to make sure that you are equipping your services with the right security. The whole cryptosystem makes your data secure by encrypting and decrypting the information keys differently at both parties (the client and the server).

As mentioned above, TLS 1.3 is a hybrid cryptosystem which means to encrypt/decrypt data, it uses two ways of cryptography: Public-key cryptography & Private-key cryptography. Public-key cryptography offers the encryption of free, open, and most of the time huge information keys for users which is also an expensive way of encryption. Private-key cryptography only works for the owner of it and it is a very safe way to decrypt the content. Here comes one of the features of TLS 1.3 that makes it all cheaper, faster, and also fully secure. TLS 1.3 uses Public-key cryptography to make it convenient for the user to establish the connection and after that, it uses Private-key cryptography to make the content/data be used securely.

As a business owner, you want to make deals, hold meetings, events, and deliver your products and services to your customers as soon as possible. You already know that TLS 1.3 is fast, but when we say that word what do we mean by it? When a deal is done and both parties are happy, they usually shake hands after signing the contracts. When a user opens his/her browser and searches for your website, the whole process of data exchange, encryption, and the other things we talked about is called "handshakes". You should be acknowledged that each website has got a certificate which is proof that this property and this package of data has got an authenticated owner. When we look at the handshake happening between the client and your website's server, many things have got to be checked, transported, and encrypted; and one of those things is verifying your website’s certificate. TLS 1.3 not only abbreviates this process without terminating any necessary verification but also does it very quickly.

You could see why you should get equipped with TLS 1.3 when you find out how this technology got polished and published. It was a long road (5 years) for developers at IETF (Internet Engineering Task Force) to develop TLS 1.3 after TLS 1.2 and improve it to its best potentials. They wanted TLS 1.3 to become the ultimate security protocol for any website’s data transportation. Since they wanted it to be published and to be used widely; so, they made it from scratch and abandoned TLS software backward compatibility for the sake of ultimate security.

We, at ArvandCloud services, are here to provide you with the best services available to secure your content and to become the bridge with the very strict foundations to give your customers assurance of making their privacy your priority. If you want to secure the handshakes happening between you, your colleagues, and your clients with TLS 1.3, we are here at your service.

Written by Tarokh Tarhandeh

June 29th, 19