**Always use TLS for REST APIs**

**Every web API should use TLS (Transport Layer Security)**. TLS **protects the information our API sends** (and the information that users send to your API) **by encrypting the messages while they’re in transit**. We might know TLS by its predecessor’s name, SSL. We’ll know a **website has TLS enabled when its URL starts with https://** instead of http://.

**Without TLS**, a **third party could intercept and read sensitive information in transit**, like API credentials and private data! That undermines any of the authentication measures we put in place.

**TLS requires a certificate issued by a certificate authority**, which also **lets users know that the API is legitimate and protected**. Most cloud providers and hosting services will manage the certificates and enable TLS for us. If we can, **let our host manage the certificates for us**—it means no hassle at all and **every API call will be automatically secured**.