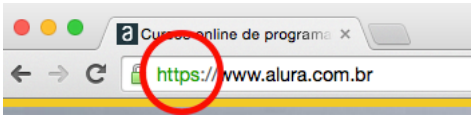
03

Funcionamento do HTTPS

Transcrição

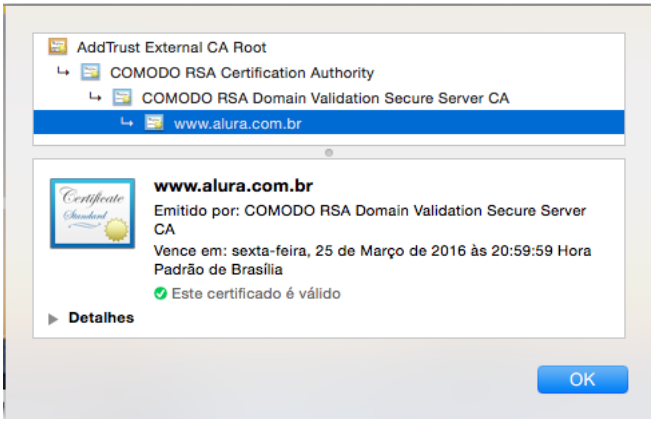
Ao acessarmos o site da Alura (https://www.alura.com.br) pelo navegador podemos perceber que ele já usa o protocolo **HTTPS**:



Reparem que no navegador, ao lado do `https` , aparece um cadeado e que ao clicarmos no cadeado podemos ver mais informações sobre HTTPS. Uma dessas informações indica que a Alura tem uma identidade confirmada. O que isso quer dizer?

O HTTPS para garantir segurança usa criptografia baseada em chaves públicas e privadas e para gerar essas chaves publicas e privadas é preciso garantir a identidade de quem possui essas chaves e isso é feito a partir de um **certificado digital**, ou seja, um certificado digital é utilizado para **identificar** determinada entidade e ainda é utilizada para geração das chaves de criptografia.

Apesar disso, ainda é necessário que uma **autoridade certificadora**, que nada mais é que um órgão ou entidade confiável, garanta não apenas a identidade do site mas também a validade do certificado. No caso da Alura a autoridade certificadora é a *COMODO RSA Domain Validation*, mas existem outras.



Dito isso, como tudo funciona? Os navegadores em posse da chave pública criptografam as informações e as enviam para o servidor que as descriptografa com a chave privada. É importante notar que apenas a chave privada descriptografa as informações criptografadas com a pública, e também que deve-se manter a chave privada segura.

O que aprendemos nesse capítulo?

- Só com **HTTPS a web é segura**.
- HTTPS significa usar um **certificado digital** no servidor.
- O certificado prova a **identidade** e tem **validade**
- O certificado possui uma **chave publica**.
- A chave é utilizada pelo navegador para criptografar os dados.