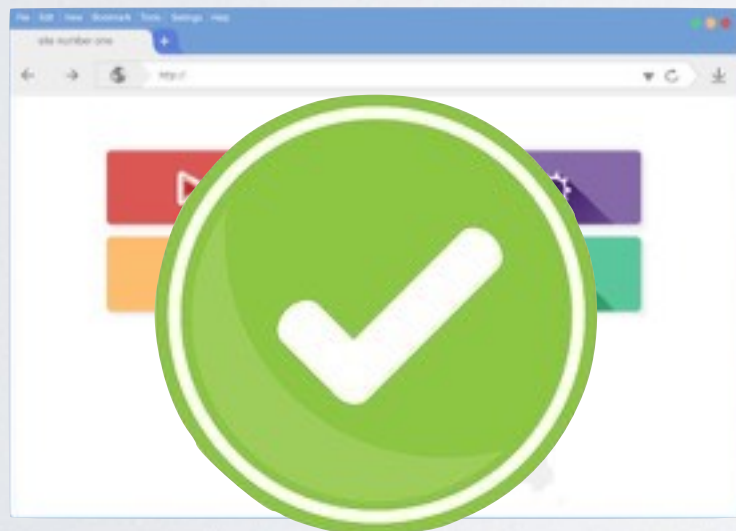


HTTPS

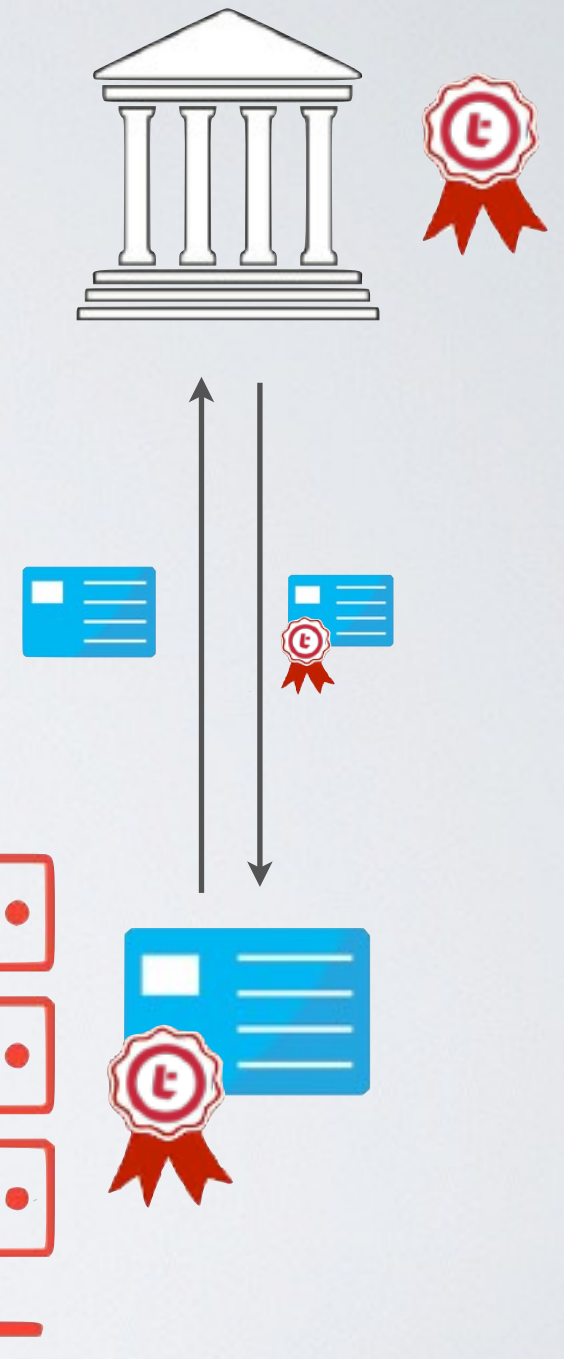
Certificate Authority (CA)



TLS Handshake



AE Session



HTTPS in practice

The Web Application owner must

1. Acquire a domain name through a *Domain Name Registrar*
2. Configure the DNS to associate the domain name with IP address of the server
3. Generate a certificate and request the *Certificate Authority* to sign it
 - ➡ The CA will verify the domain ownership
 - ➡ The certificate must be renewed periodically (usually every year)