Enhancing the User Experience with Client Security Context

Brian Noyes
CTO, SOLLIANCE INC

@briannoyes www.briannoyes.com

Module Overview

Enabling Silent Renew of Your Access Tokens

Providing a Security Context for Your Client Code

Enhancing the User Experience Using the Security Context

Single Sign-On Across Applications

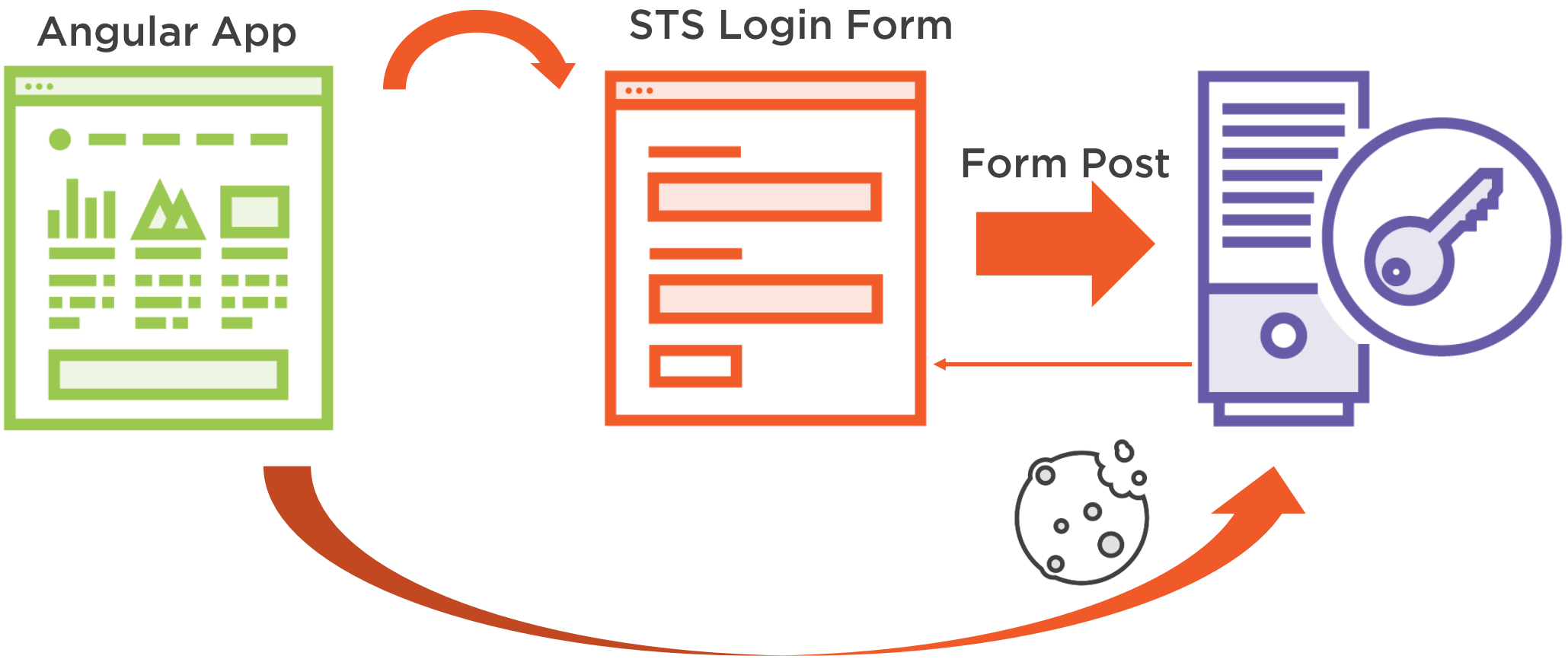
Access tokens expire

Once expired, calling a protected API results in 401 Unauthorized

Need to obtain a new token to continue calling APIs

Can’t use OAuth 2 refresh tokens with Implicit Flow

STS Authentication Session



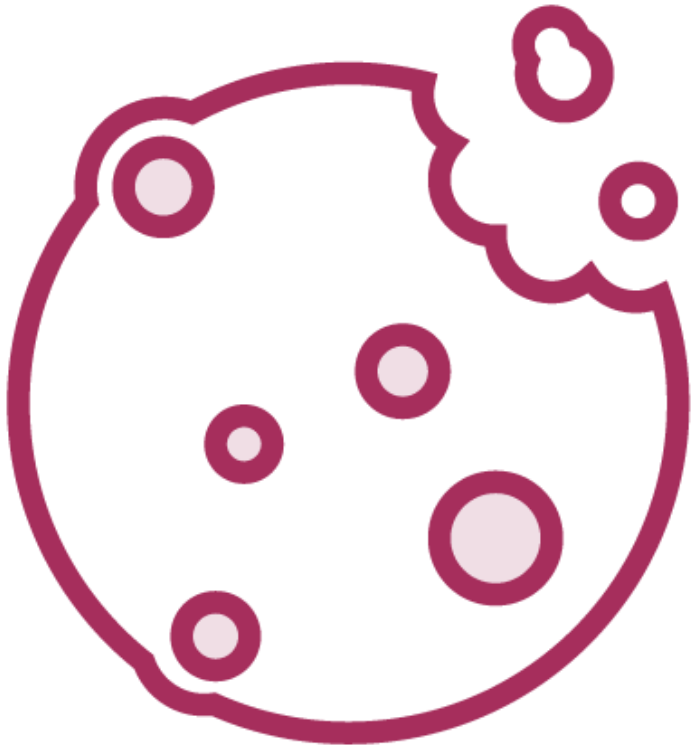
Cookie-based Authentication

Requires server side processing and rendering

Only work for single site, so no Single Sign-On (SSO)

Require attention to protect against CSRF and XSS

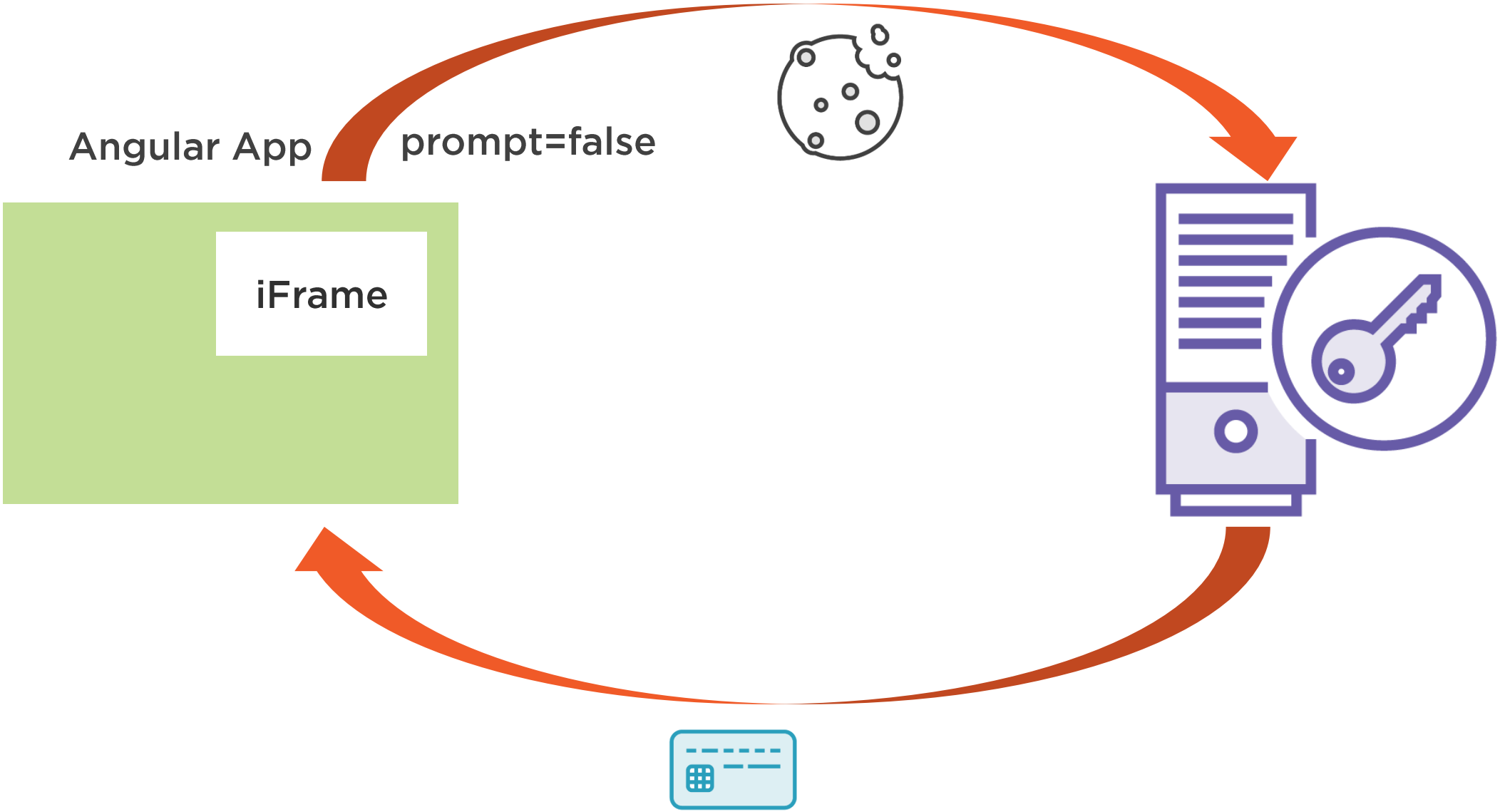
HTTP Only Cookies



Not accessible to client side JavaScript

Harder to hijack

STS Authentication Session



Summary

- Angular security big picture
- Authenticating users with OpenID Connect
- IdentityServer4 & Auth0
- Authorizing API calls with OAuth 2 access tokens
- Use oidc-client to handle all the protocol details for you
- Keeping login sessions alive with silent renew
- Customizing the user experience based on security context