Encrypted Token Pattern CSRF Defence

10. API decrypts token

9. AJAX request includes token in HTTP Header

11. Key is confirmed, Timestamp has not expired

AJAX

8. Browser invokes AJAX request

12. Proceed to step #3

Token

1. User sends a successful login request

2. Web Server invokes API

Login

Browser

Token

Router

Web Servers

API

6. Web Server returns the Token

Token

Devices

Hidden Field

3. API generates a large random number (nonce)

7. Token is stored in a hidden field

4. API encrypts a key combined with the nonce value, the user's ID, and a Timestamp

5. API formats the encrypted value in a Token

Paul Mooney