OAuth Cheat Sheet

José Catalán Tatay
and Szymon Drosdzol

CONTENT

Checklists

DOYENSEC

OAuth Client Checklist

- [ ] 01 Is all communication encrypted (i.e., TLS/HTTPS)?
- [ ] 02 Is the proper flow used?
  - [ ] 02.1 Authorization Code flow, when client credentials can be kept secret (mainly for classic web applications), PKCE extensions should be added when possible too
  - [ ] 02.2 Authorization Code flow with PKCE, when client credentials cannot be kept secret (Single Page Applications, Mobile Applications, Desktop Applications, etc.)
- [ ] 03 Are the client credentials protected?
- [ ] 04 Is the flow protected against CSRFs with a nonce in the state parameter?
- [ ] 05 Is the allowed redirect_uri fully under developer control (i.e., ensure there are no dangling domains)
- [ ] 06 The callback endpoint does not include any external content (scripts, img, css, etc.) in the page and it instantly redirects the user to the landing page. If the inclusion of external content is required, configure the Referrer-Policy header such that the querystring is not included: Referrer-Policy: origin
- [ ] 07 For Android Applications, is the callback URL using a Verified Android App Link?
- [ ] 08 Is the Resource Owner identified based on the sub field?
  - [ ] 08.1 Are Resource Owners identified based on a field that is immutable and not controllable by attacker?
- [ ] 09 For Authorization Code flow with PKCE: is the S256 transformation method (t_m) used instead of plain?

DOYENSEC

OAuth Server Checklist

01 Is all communication encrypted (i.e., TLS/HTTPS)?

02 Are client secrets protected?

03 Are client secrets verified?

04 Is the redirect_uri properly validated using a strict byte-for-byte comparison? (i.e., exact urls: not domains, subdomains, wildcards, query parameters, etc.)

05 Are authorization codes short lived?

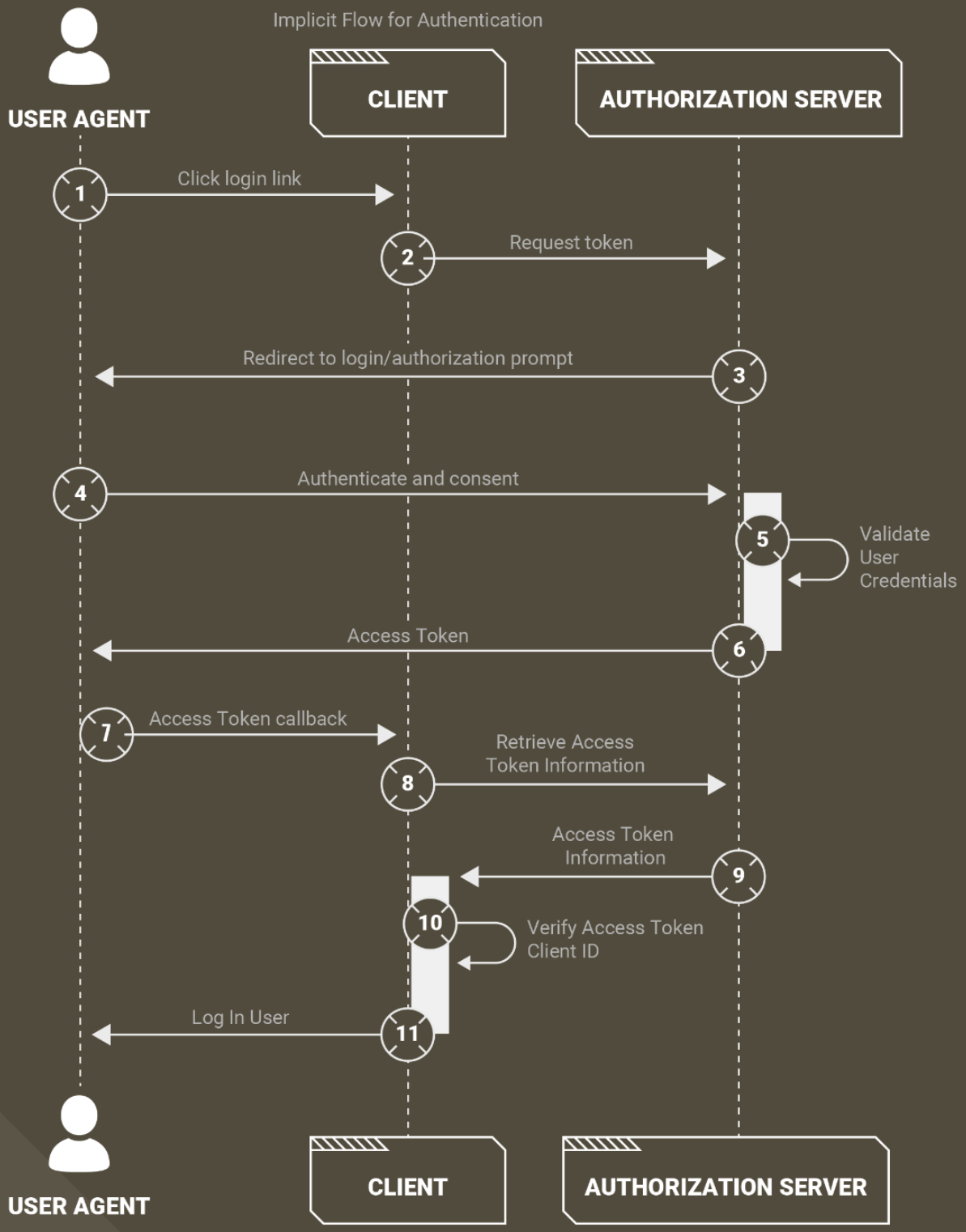
06 Are authorization codes invalidated after use? If an authorization code is used more than once, the authorization server must deny the request and should revoke all tokens previously issued based on that authorization code.

07 Can scope be changed after user's consent?

Basic Flows

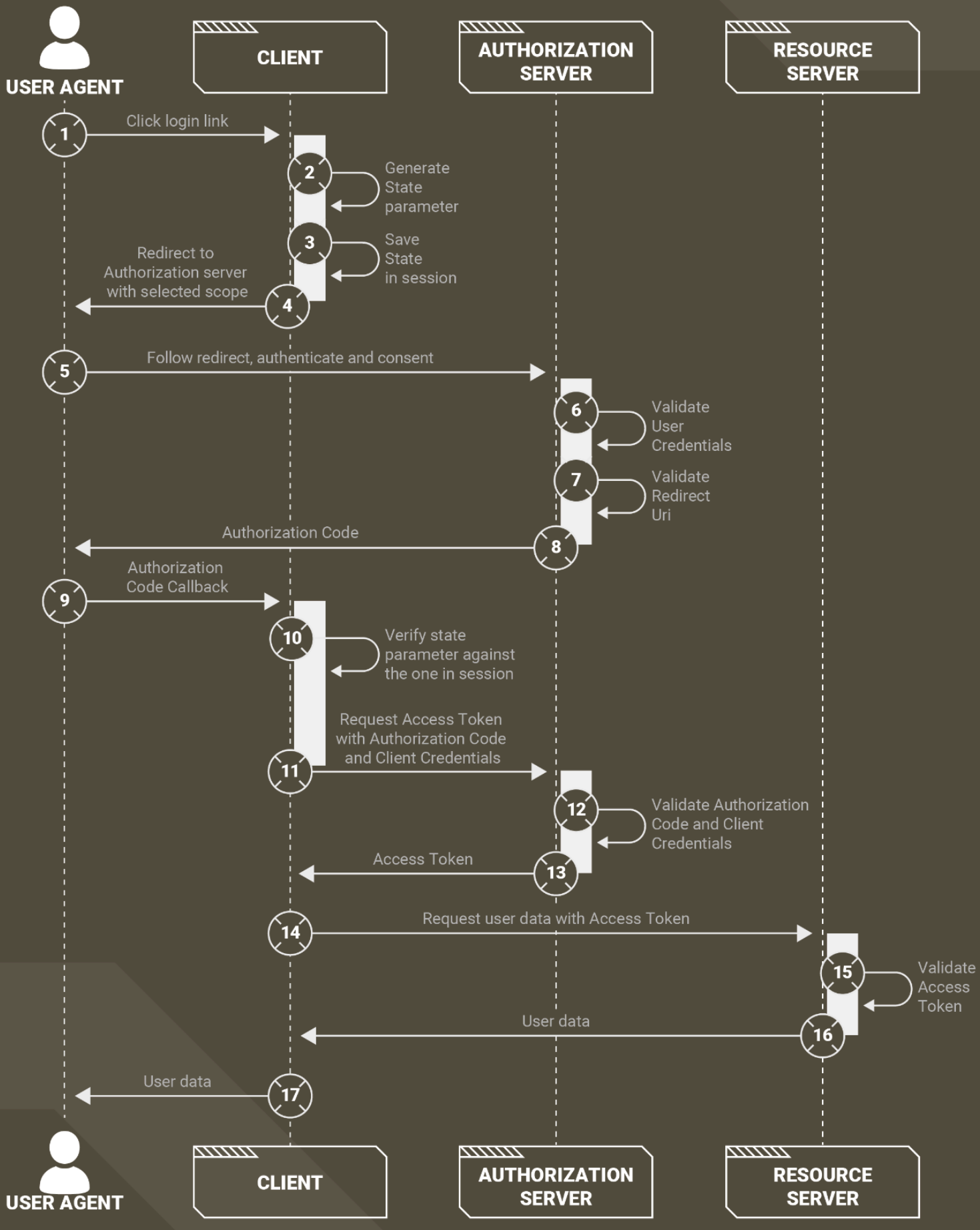
DOYENSEC

Implicit Flow



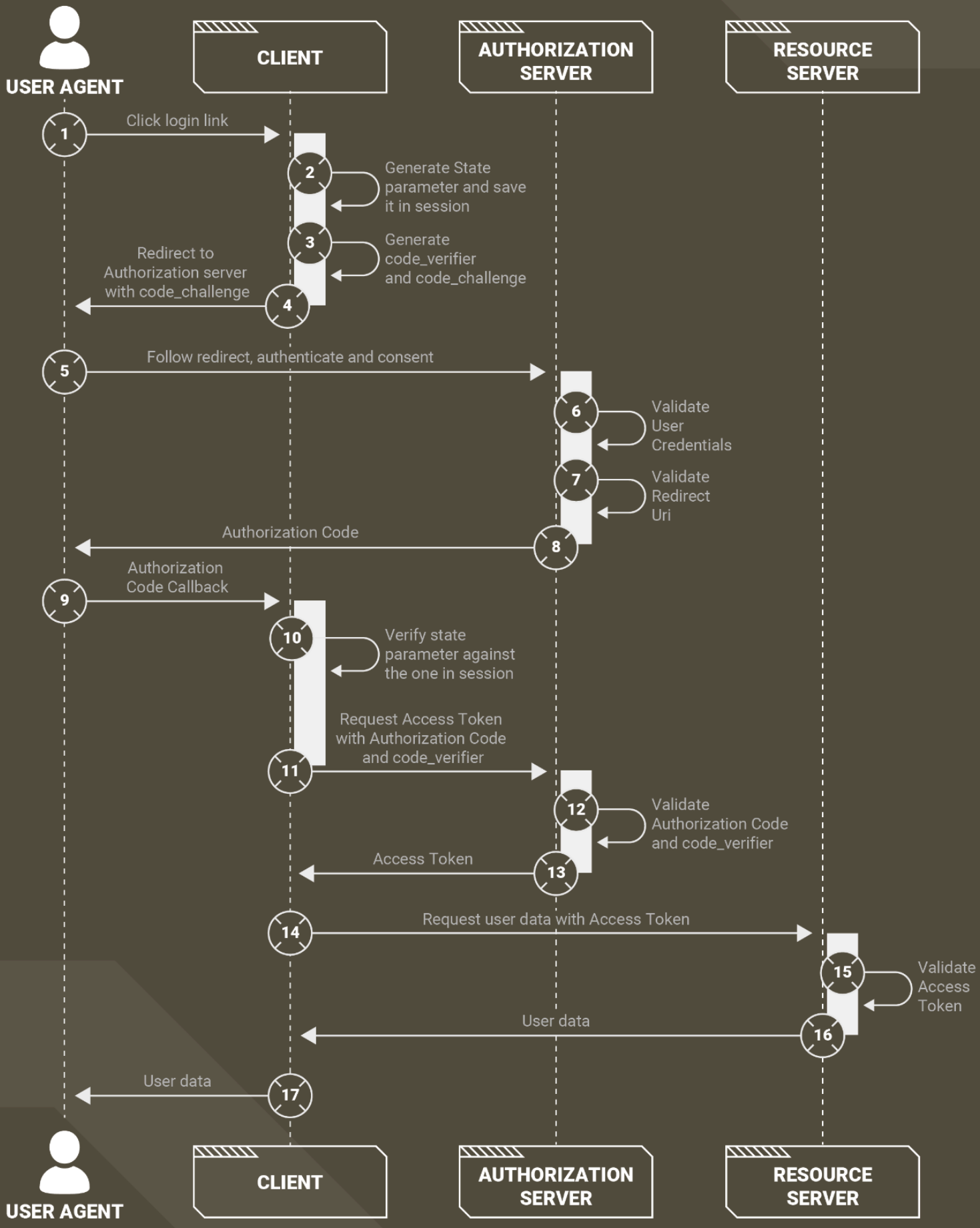
DOYENSEC

Authorization Code Flow



DOYENSEC

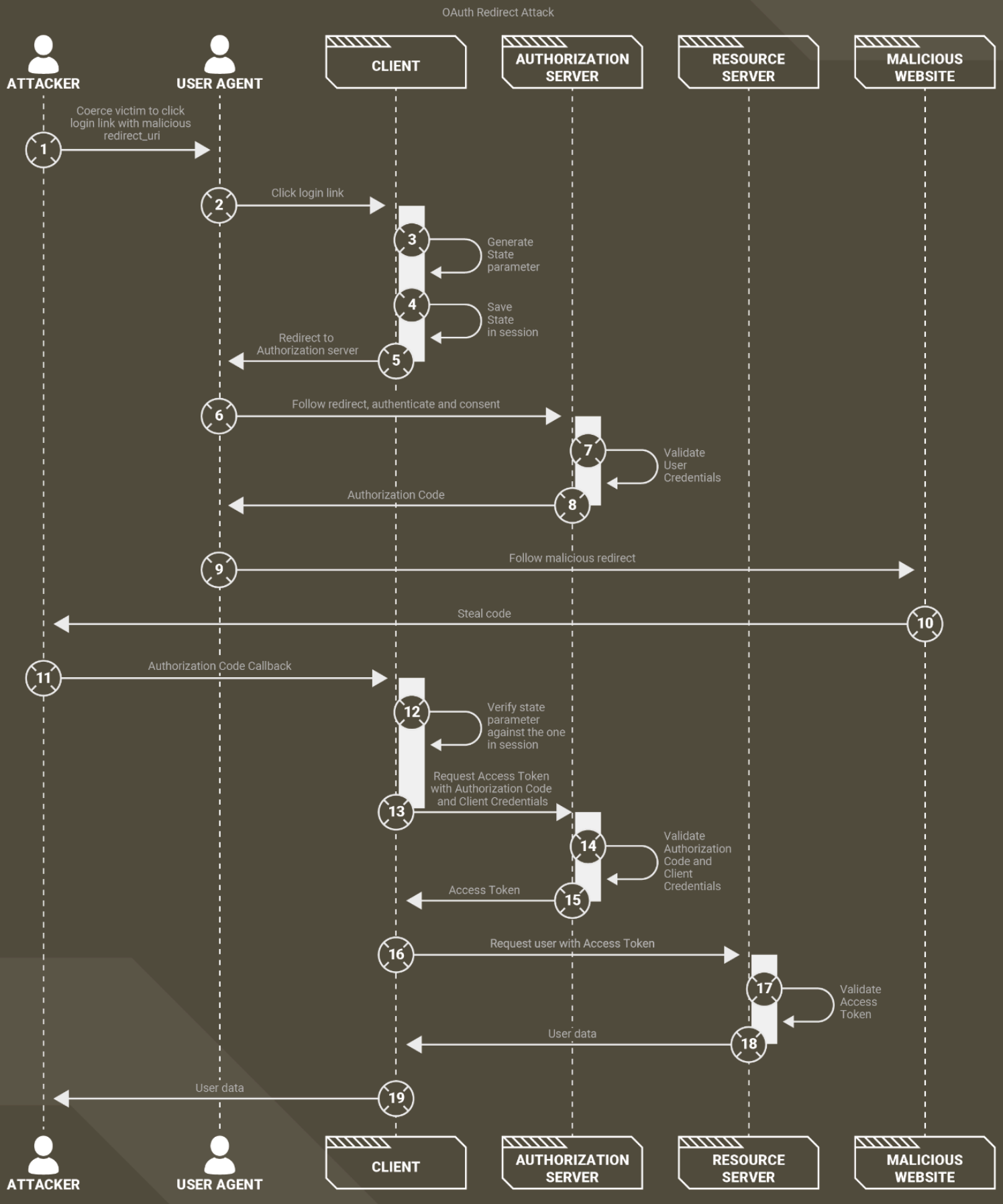
Authorization Code Flow with PKCE



Basic Attacks

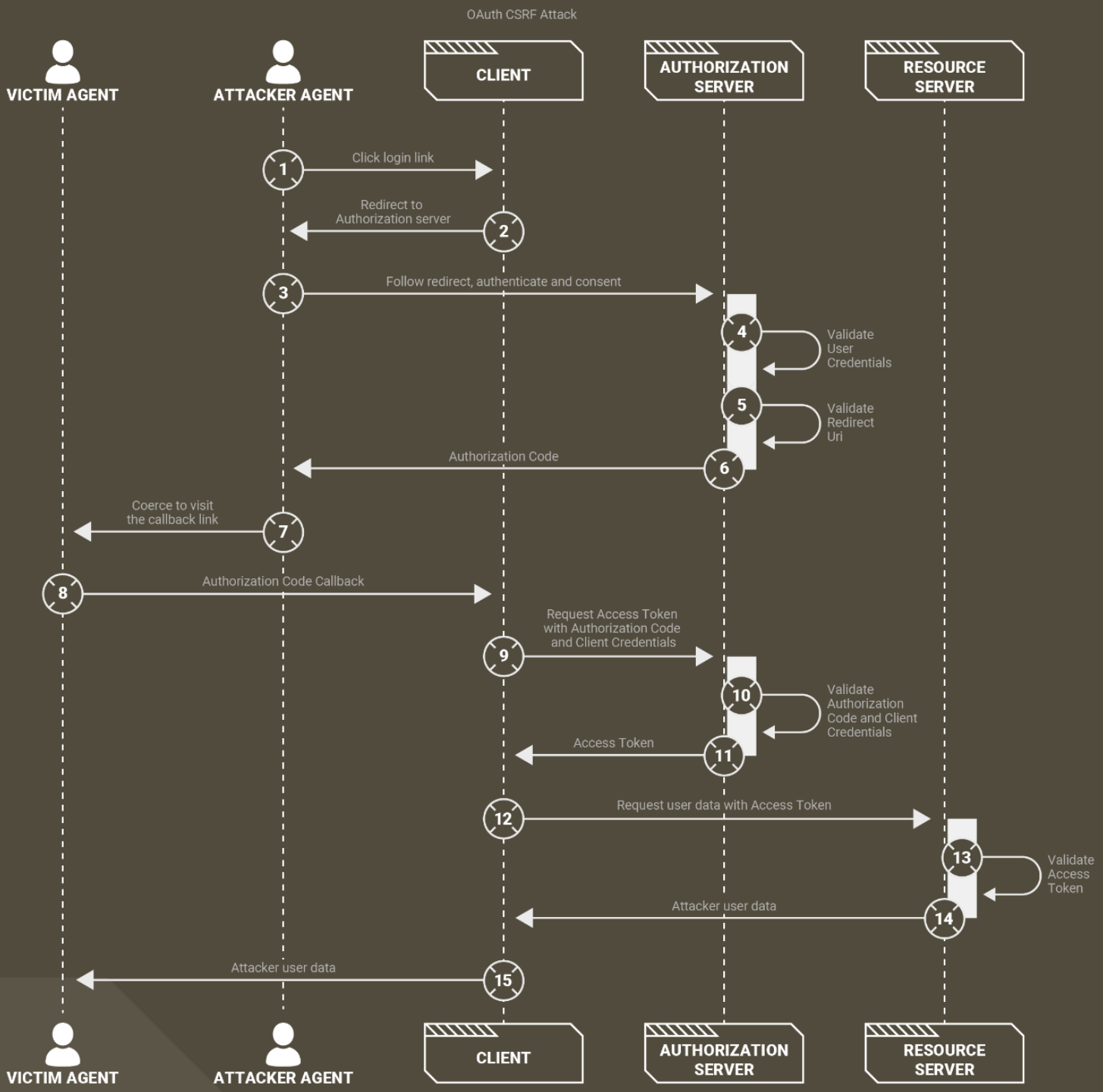
DOYENSEC

Redirect Attack



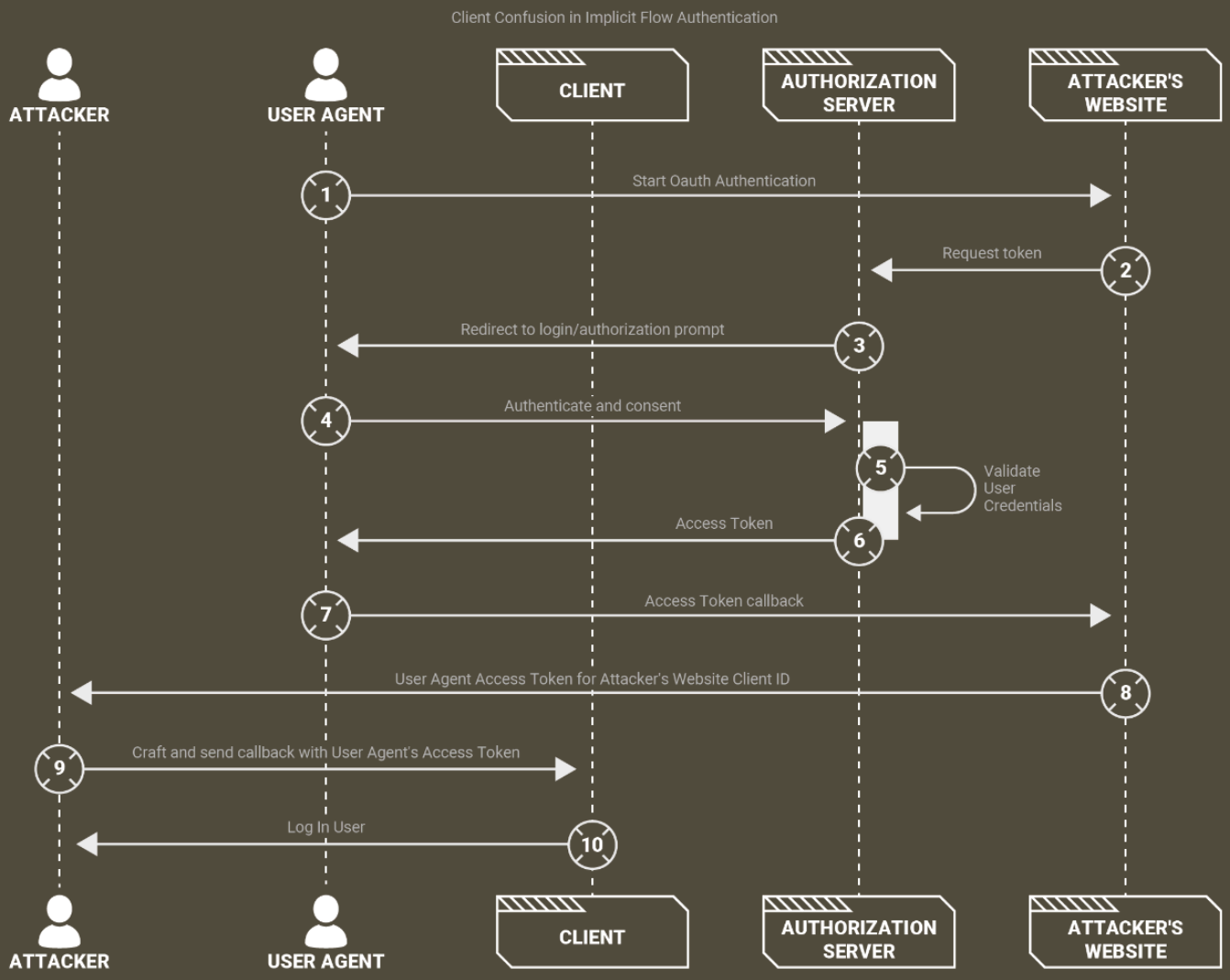
DOYENSEC

CSRF attack



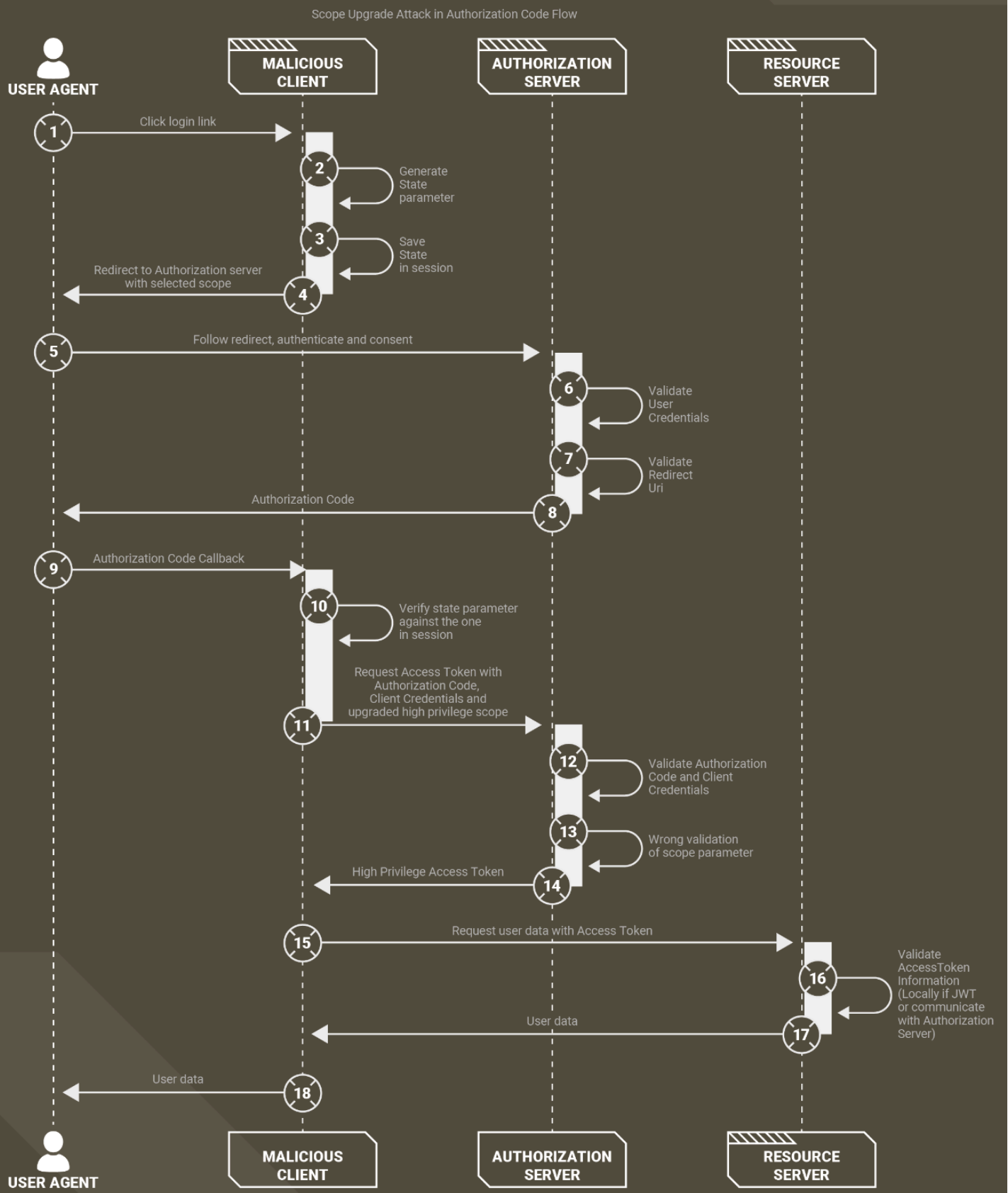
DOYENSEC

Client Confusion Attack



DOYENSEC

Scope Upgrade Attack



About Doyensec

About Doyensec

https://www.doyensec.com

Doyensec was founded in 2017 by John and Luca who are its only stakeholders. The company exists to further the passion and focus of its creators. We aim to provide research-driven application security, enabling trust in our client's products and evolving the resilience of the digital ecosystem.
With offices in the US and Europe, Doyensec has access to a unique talent pool of security experts capable of providing worldwide consulting services.
We keep a small dedicated client base and expect to develop long term working relationships with the projects and people involved. We will find bugs, but we know that is just the first step in the process. At any stage of your security maturity, you can rely on Doyensec to solve your unique application security needs.
We value and rely on the following principles:

Passion.

We believe quality comes from passion and care. We love what we do, and continuously work on mastering our craft. Every engagement is finely executed with dedication and attention to details.

Expertise.

Our team has decades of experience in application security. We are industry leaders in penetration testing, reverse engineering, and source code review. Doyensec researchers have discovered numerous vulnerabilities in widely-deployed products, secured Fortune 500 enterprises, advised startups and worked with tech companies to eradicate security flaws.

Focus.

Security craftsmanship is all about individual attention and delivering tailored security services and products. We concentrate on application security and do fewer things, better.

Research.

The fast changing landscape of technologies and security threats requires constant innovation. We are dedicated to providing research-driven application security and therefore invest 25% of our time in building security testing tools, discovering new attack techniques and developing countermeasures.


DOYENSEC