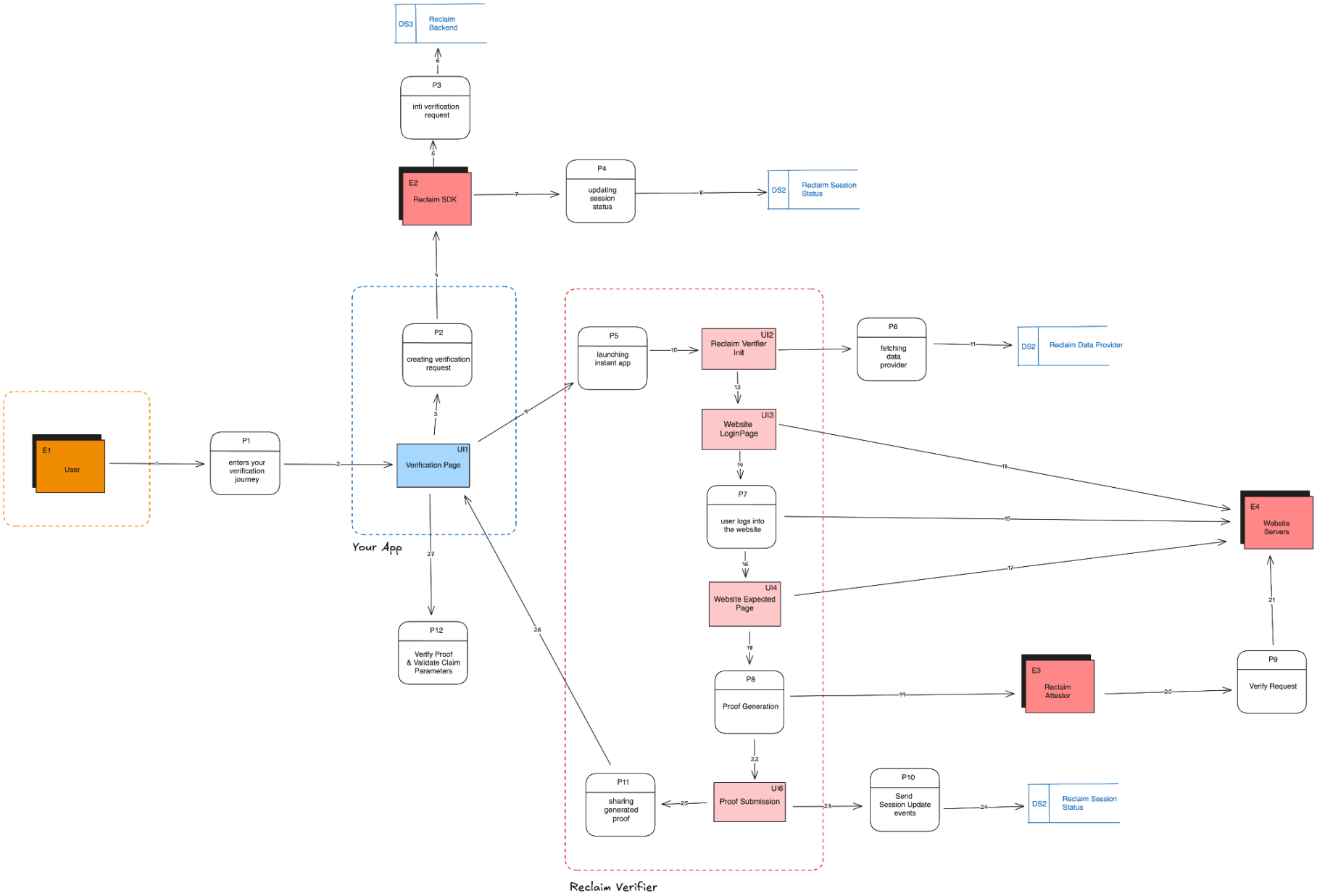
Verification Journey Data Flow Diagram

This document provides information about a user's Reclaim data verification journey using a Data Flow Diagram.

In this document, 'you' refers to the developers who are consuming the Reclaim Protocol products like the Reclaim SDKs to request data from a user.

This document details the data flow depicted in the "Data Flow" diagram, visually representing a secure attestation process between Your App, User, Attestor, Reclaim Verifier and Website. The process ensures the integrity and confidentiality of data exchanged, leveraging TLS encryption and Zero-Knowledge Proofs (ZKPs).


DS3
Reclaim Backend
P3
inti verification request
E2
Reclaim SDK
P4
updating session status
DS2
Reclaim Session Status
P2
creating verification request
E1
User
P1
enters your verification journey
UI1
Verification Page
Your App
P5
launching instant app
UI2
Reclaim Verifier Init
P6
fetching data provider
DS2
Reclaim Data Provider
UI3
Website LoginPage
P7
user logs into the website
UI4
Website Expected Page
E4
Website Servers
P12
Verify Proof & Validate Claim Parameters
P8
Proof Generation
E3
Reclaim Attestor
P9
Verify Request
P11
sharing generated proof
UI6
Proof Submission
P10
Send Session Update events
DS2
Reclaim Session Status
Reclaim Verifier

Explanation

Starting with the outer swimlanes (User, Attestor, Website) and moving inwards:

1. **User to Website (TLS Handshake):** User initiates a secure connection with the Website via TLS.
2. **Website to User (TLS Handshake):** Website responds, establishing the secure TLS connection.
3. **Website to Attestor (Forward TLS Client Handshake):** Website forwards the User's TLS handshake to the Attestor for authentication.
4. **Attestor to Website (Forward TLS Client Handshake):** Attestor processes the handshake and forwards it back to the Website.
5. **Attestor to Website (TLS Server Handshake):** Attestor initiates its own TLS handshake with the Website.
6. **Website to Attestor (TLS Server Handshake):** Website completes the TLS handshake with the Attestor.
7. **Website to User (Forward TLS Server Handshake):** Website forwards the Attestor's TLS handshake to the User.
8. **User to Website (Forward TLS Server Handshake):** User completes the TLS handshake with the Website.

Moving to the "Encrypted Request" section:

9. **User to Website (Encrypted Request):** User sends an encrypted request (containing private/public parts and key updates) to the Website.
10. **Website to Attestor (Transfer Encrypted Request):** Website transfers the encrypted request to the Attestor.
11. **Attestor to Website (Forward Encrypted Response):** Attestor processes the request and sends an encrypted response back to the Website.
12. **Website to User (Forward Encrypted Response):** Website forwards the encrypted response to the User.

Entering the "Detect and Reveal" section:

13. **User to Detect and Reveal (Detect Part to be Revealed):** The user specifies the part of the response they want to reveal.

Moving to the "Verification" section:

14. **Detect and Reveal to Verification (Create ZK Proof):** The "Detect and Reveal" component triggers the creation of a Zero-Knowledge (ZK) proof in the Verification component.

15. **Verification to User (Reveal Part, Redacted Ciphertext, Plaintext, ZK Proof):** The Verification component sends the revealed part, redacted ciphertext, plaintext, and ZK proof to the User.
16. **Verification to Attestor (Verify ZK Proof):** The Verification component sends the ZK proof to the Attestor for verification.
17. **Attestor to Verification (Check Revealed Part of Request and Response):** Attestor checks the revealed part of the request and response against its own records.
18. **Attestor to User (Signed Proof):** Attestor sends a signed proof of verification to the User.

Returning to the outer swimlanes:

19. **User receives TLS handshake data from Website (implied from steps 2 and 8).**
20. **Attestor receives TLS handshake data from Website (implied from steps 3 and 5).**
21. **Website receives TLS handshake data from Attestor (implied from steps 5 and 6).**
22. **Website receives encrypted request from User (step 9).**
23. **Attestor receives encrypted request from Website (step 10).**
24. **Attestor sends encrypted response to Website (step 11).**
25. **Website sends encrypted response to User (step 12).**
26. **User sends data to "Detect and Reveal" (step 13).**
27. **User receives signed proof from Attestor (step 18).**

For more information, please visit [Reclaim Protocol]