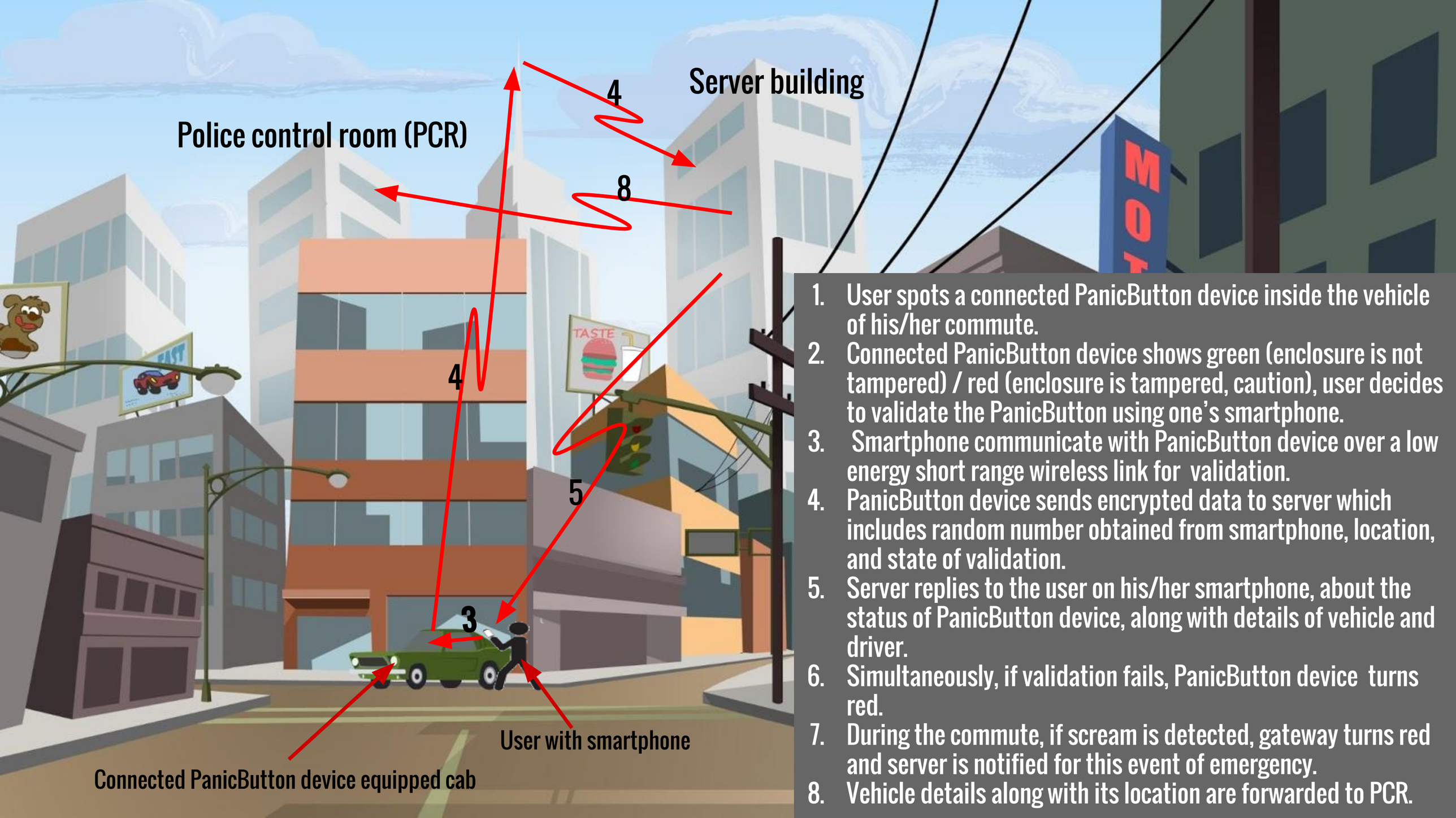

1. User spots a connected PanicButton device inside the vehicle of his/her commute.
2. Connected PanicButton device shows green (enclosure is not tampered) / red (enclosure is tampered, caution), user decides to validate the PanicButton using one's smartphone.
3. Smartphone communicate with PanicButton device over a low energy short range wireless link for validation.
4. PanicButton device sends encrypted data to server which includes random number obtained from smartphone, location, and state of validation.
5. Server replies to the user on his/her smartphone, about the status of PanicButton device, along with details of vehicle and driver.
6. Simultaneously, if validation fails, PanicButton device turns red.
7. During the commute, if scream is detected, gateway turns red and server is notified for this event of emergency.
8. Vehicle details along with its location are forwarded to PCR.