**Assumptions:**

1. PoC covers only smart watches, utilization option with other smart devices need to be considered separately
2. Online payment mechanism
3. Android

**User case 1: User performs first payment with smart watch**

**Primary actor:** user

**Scope:**

**Level:**

**Actors definition:**

**User** – to get payment transaction in the easiest and the quickest way

**Customer Payment System** – perform payment transaction at a high security level

**SDK System (‘Smart Login’)** – SDK to be built in Customer Payment System

**Smart Watch app** – secure data storage of Client’s information

**Mobile app** – payment system mock-up (for ex., login into mobile banking, mobile payment engine)

**Precondition:** ?

**Minimal guarantees:**

* Mobile
* Active Smart watch
* Access to internet

**Success guarantees:** transaction is performed, security is kept

**Trigger:** User wants to make payment transaction

**Main success scenario:**

1. **User** clicks on ‘Buy’ button in opened Mobile app (only mobile? No website?)
2. **Mobile app** propose User to ‘Perform payment in one click with your smart watch, your key authorization’, display buttons ‘Ok’ and ‘Skip’ (what criteria smart watch must satisfy to be successfully paired?)
3. **User** clicks ‘Ok’ on mobile device
4. **Mobile App** detects smart watch
5. **Mobile App** asks User to enter ‘password’ and ‘confirm password’ (Master Password, what criteria password must meet?) to pair Smart Watch with Mobile
6. **User** enters ‘password’ and ‘confirm password’ (Master Password)
7. **Mobile App** checks entered password compliance (what criteria we must check?)
8. **Smart Watch app** asks User to confirm pairing of wearable and mobile app by tapping on smartwatch (if several watches are nearby our user?)
9. **User** taps on ‘Pair’ button on smart watch
10. **Mobile App** performs pairing with Smart watch
11. **SmartWatch App** and **Mobile App** notify of successful pairing (mobile and smartwatch)
12. **Mobile App** sends ‘Password’ to **SDK System** (or SDK system need to get the password from Mobile App?)
13. **SDK System** creates Key from ‘password’, divides Key into 2 parts, sends 1st part to **Mobile App** and 2nd part to **Smart Watch App**
14. **Mobile App** receives and saves 1st part of Key (where the key is saved?)
15. **Smart Watch App** receives and saves 2nd part of Key (where the key is saved?)
16. **Mobile App** display ‘Confirm purchase’ and ‘Cancel’ button and requests from user to confirm purchase order.
17. **User** click ‘Confirm purchase’ on mobile
18. **Smart Watch app** and **Mobile app** notify SKD system of potential payment transaction (What system informs SDK system?)
19. **SDK System** requests and receive passwords from **Smart Watch app** and **Mobile app**
20. **SDK System** merge passwords in one key
21. **SDK System** check key compliance (what we must check here?) and confirm user authorization
22. **Mobile App** display ‘Payment was successful’.

**Extension:**

2a. User click ‘Skip’: Mobile app performs general payment procedure with card info, card confirmation procedure

4a. Smart watch is not activated, turned off/discharged: Mobile app notify ‘Your smartwatch was not detected, please activate and keep it near mobile’ and display button ‘Reply’

4b. Smart watch is not on hand: is it a possible alternative case?

4c. Smart watch is ~5-10 meters away from Mobile: is it a possible alternative case?

4d. Several smart watches were detected: Mobile App display the list of detected Smart watches and ask user to select his permanent smart watch. User selects, Smart watch app ask user to confirm by tapping on smart watch

7a. ‘Password’ and ‘Confirm password’ are not the same: Mobile App displays ‘Password and Confirm password don’t match. Please enter once again’’

7b. Entered password is weak: Mobile App displays ‘Please enter password that will contain following symbols XXXXX’ and asks to re-enter ‘password’ and ‘confirm password’

10a. Pairing process was interacted, Mobile App notify ‘Something went wrong’ and displays buttons ‘Retry’ (Mobile app repeat pairing process) and ‘Go to standard payment procedure’ (Mobile app perform standard payment process)

14a. No free space on mobile: what we do here?

15a. No free space on smart device: what we do here?

16a. User clicks ‘Cancel’, transaction will be cancelled

21a. SDK system checked that key don’t meet compliance criteria, SDK cancel transaction, Mobile App displays ‘Sorry, something went wrong. Please use standard payment procedure’

**User case 2: Repeated payment with smart watch**

**Primary actor:** The Client

**Scope:**

**Level:**

**Stakeholders and Interests:**

**Precondition:** Client wants to perform payment transaction

**Minimal guarantees:** connection to internet, smart device, mobile, be a client of bank

**Success guarantees:** successful payment done, same security level with SmartLogin transaction as w/o

**Trigger:**

**Main success scenario:**

1. **User** clicks on ‘Buy’ button in opened Mobile app
2. **Mobile App** detects smart watch
3. **Mobile App** performs pairing with smartwatch
4. **Mobile App** performs smart watch compliance check (what we check here?)
5. **Smart Watch app** display buttons ‘Confirm’ and ‘Cancel’ and asks User to confirm purchase by tapping on smartwatch
6. **User** taps on ‘Confirm’ button on smart watch
7. **Smart Watch app** and **Mobile app** notify SKD system of potential payment transaction
8. **SDK System** requests and receive passwords from **Smart Watch app** and **Mobile app**
9. **SDK System** merge passwords in one key
10. **SDK System** check key compliance and perform the requested payment transaction.
11. Payment/purchase is made, **Mobile App** displays ‘Your purchase was successfully made’ (or Smart Watch App???).

**Extension:**

2a. Mobile App hasn’t detected the smart watch: Mobile App display ‘No smart watch was detected. Please make sure your smart watch is activated and is placed near mobile’ and display ‘Retry’ button

3a. Pairing was unsuccessful: Mobile App display ‘Sorry. Something went wrong with synchronization’ and display ‘Retry’ and ‘Skip to general payment procedure’

4a. SmartWatch was taken away from last smart watch transaction, Mobile App asks to confirm transaction with entering password (Master Password) – why we need to regenerate the new key for mobile and smart watch?

4a.a Mobile App checks password – do we need this?

4a.b Mobile App sends password to SDK system

4a.c SDK system created key, divides it and sends 1st part to mobile and 2nd part to smartwatch

4a.d SDK permits the transaction

5a. User clicked ‘Cancel’ button: payment transaction is cancelled, user is backed to buying button/product browsing view

5b. User didn’t click any button during XX seconds: Mobile app notify ‘Purchase was not confirmed’ and display buttons ‘Reply’ and ‘Skip’

10a. SDK System checked that key don’t meet compliance criteria: Mobile App display ‘Sorry. Something went wrong. Please reply or use standard payment procedure’.