

Lightweight Security Platform for IoT: Smart hotel use case



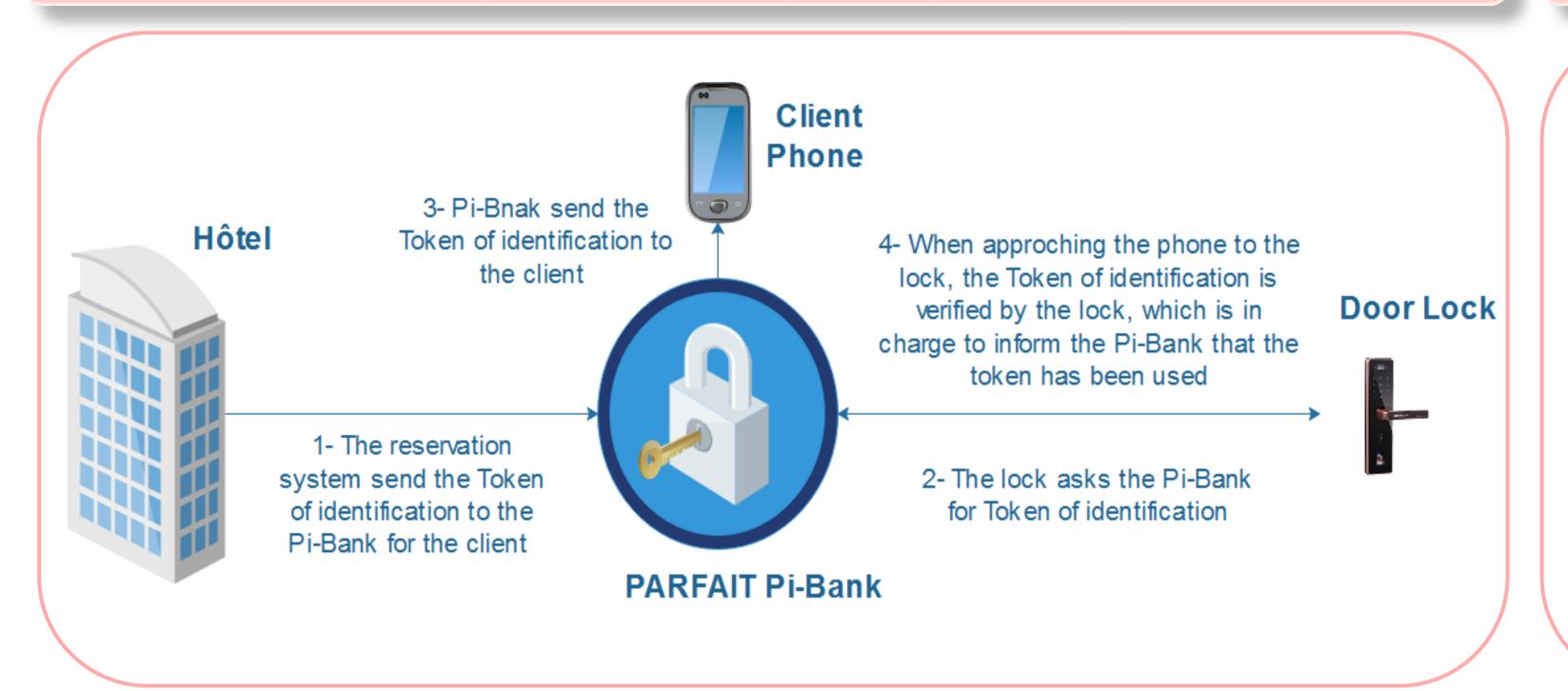
Mehdi Nacer Kerkar, Maissa Dammak, Sidi-Mohammed Senouci, Mohamed Ayoub Messous

DRIVE Lab, Univ. Bourgogne Franche Comté, F58000, Nevers France

Email: mehdi.kerkar@tuta.io, {maissa.dammak, sidi-mohammed.senouci, ayoub.messous}@u-bourgogne.fr

when adopting the Token

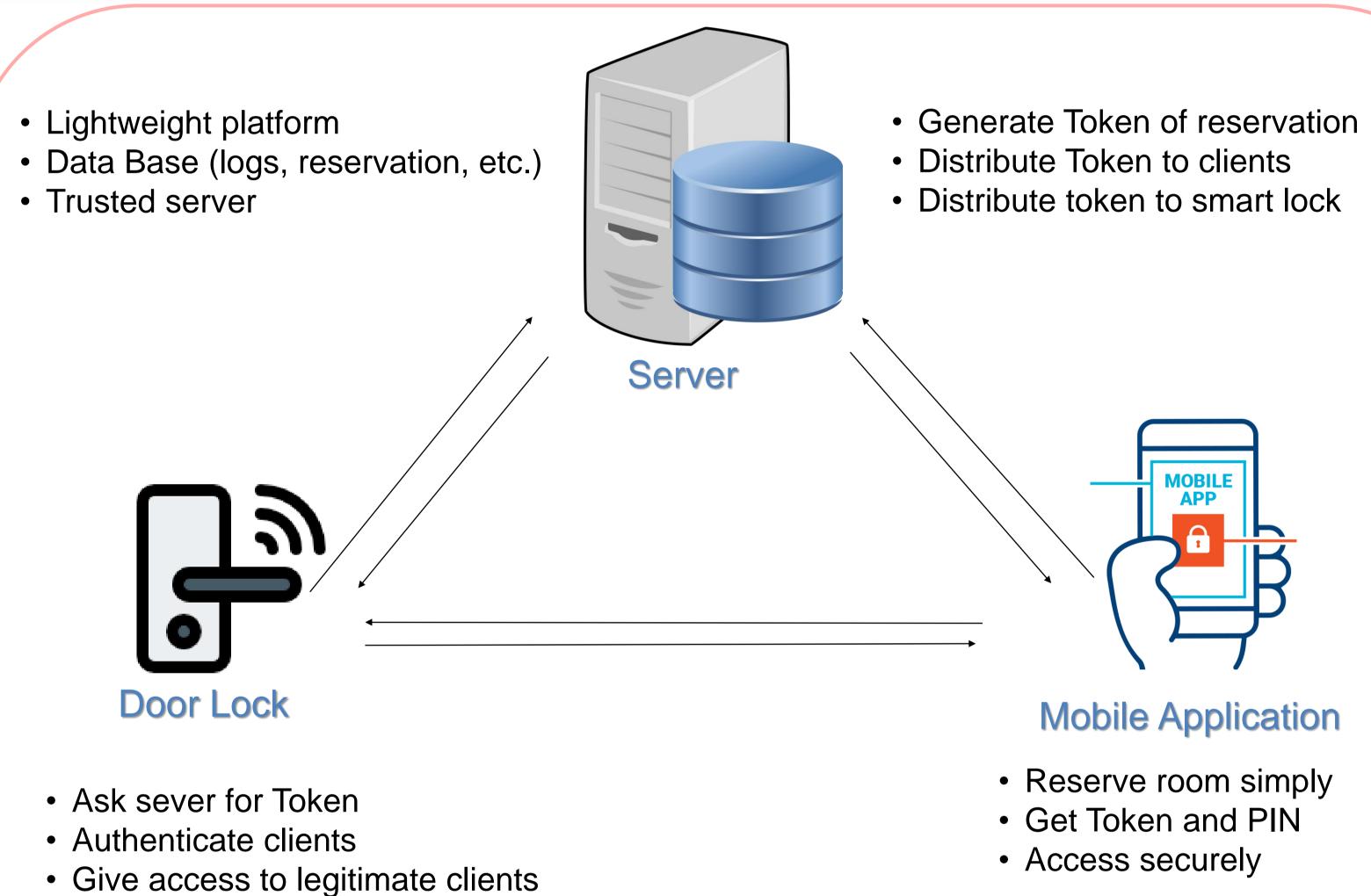
Smart hotel use case



Challenges

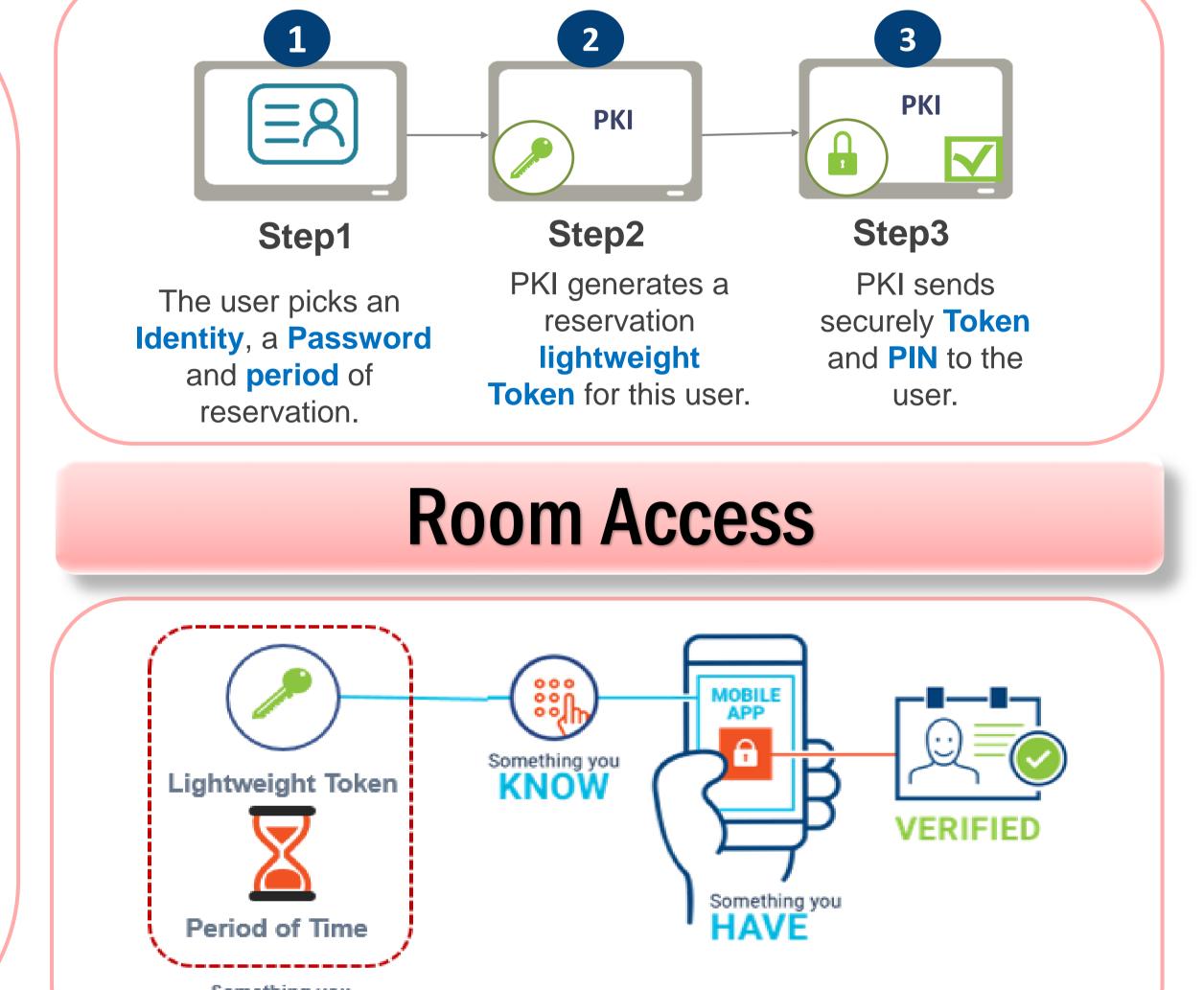


Architecture

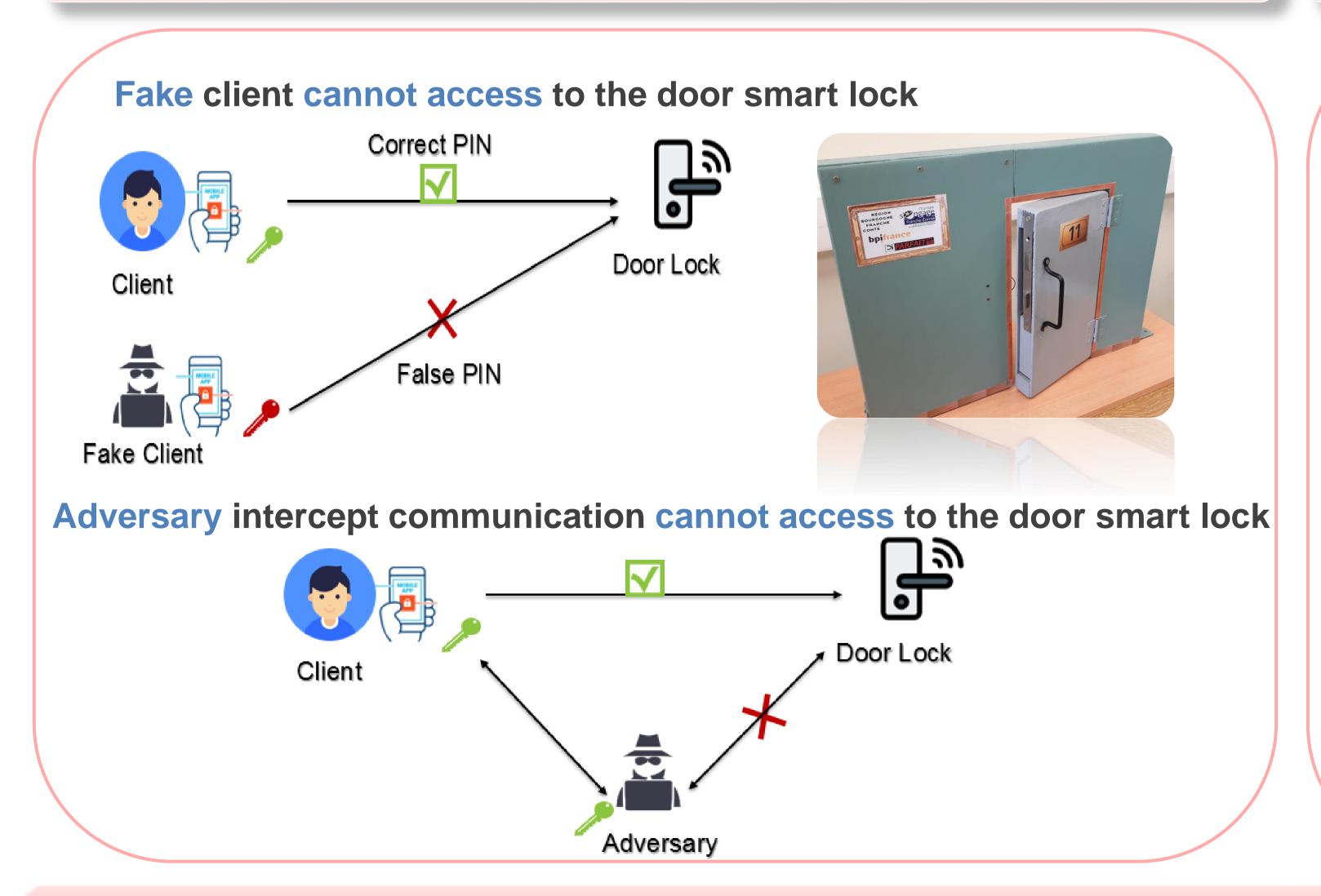


Access securely

Room Reservation



Attack Scenario

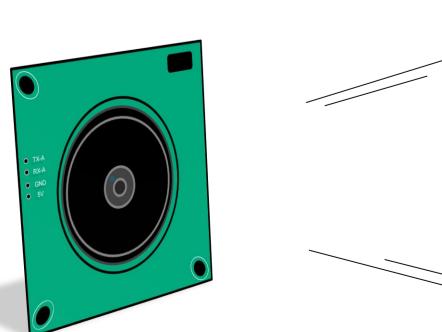


Defense Strategy

The attacker cannot generate the Token because it is randomly generated.

GET

- The attacker can eavesdrop the reservation Token but it is encrypted, so, it cannot gain access.
- The attacker can have the access pass. However, it is hashed and the hash function is irreversible.
- The attacker could not have access with the user's smartphone if he does not have the PIN code
- We can replace PIN by QRcode







Conclusion



Easy reservation and access to rooms using your personal smartphone.



The system is lightweight and ensures a secure communication among system entities.



REGION

