

Police Quarantine Violation Alert



Positive-test Patient Smarthone

Vi è installata l'applicazione per il *privacy-preserving contact tracing* che segue lo standard DP3T. Il meccanismo di rilevamento della violazione della quarantena affianca le normali routine previste da DP3T.



Smart Beacon

Beacon dotato di trasmissione Bluetooth e di logica interna capace di effettuare la codifica a chiave simmetrica (CCA sicura) di un messaggio *M* in *C*.

- ID_{beacon}: indirizzo Bluetooth del Beacon

- SK_{beacon}: chiave privata usata per cifrare

M : orario (tipo da definire)

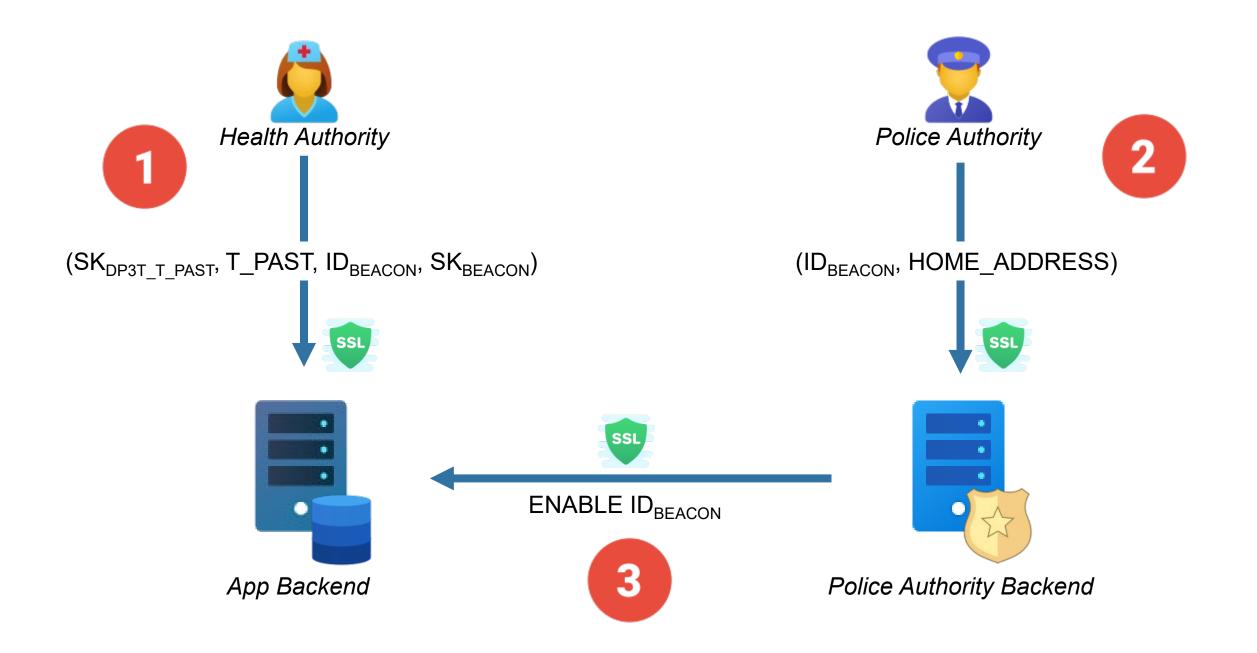
- C: messaggio cifrato

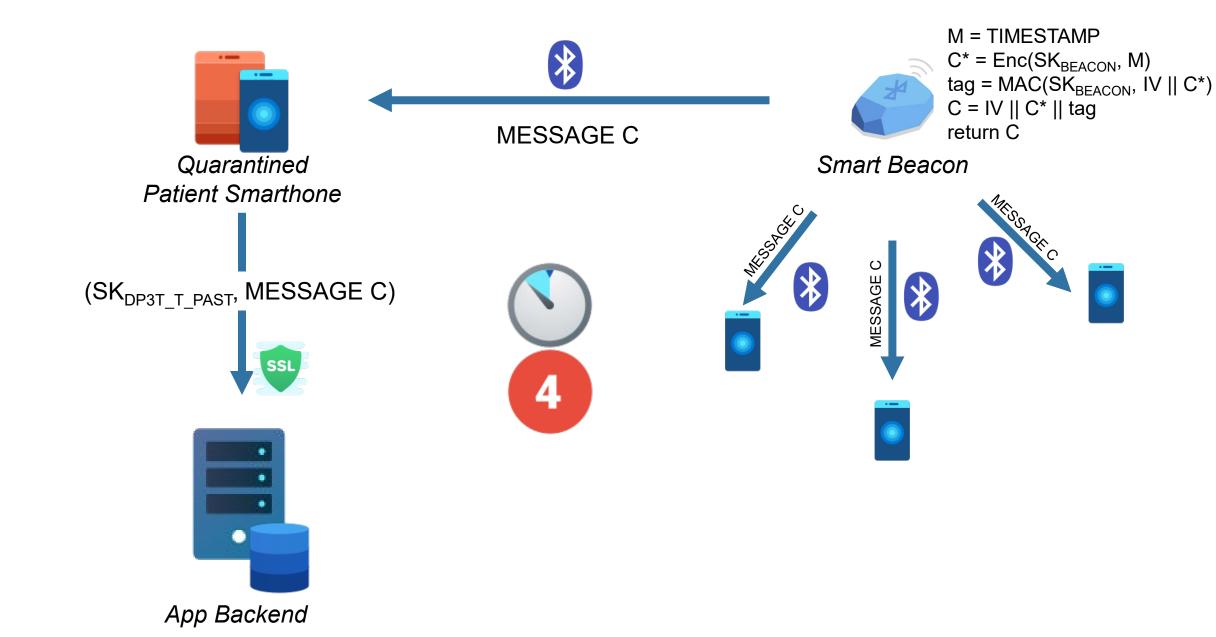
Il Beacon invia periodicamente in broadcast il messaggio cifrato C.

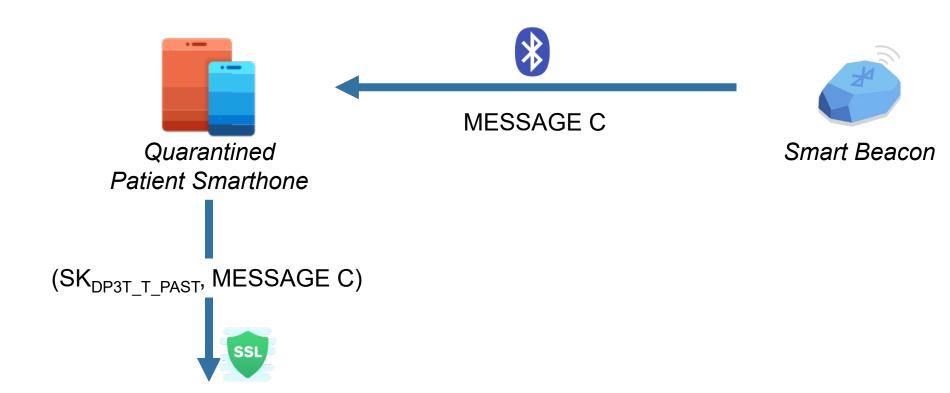


Police Authority

Provvede all'installazione dello Smart Beacon presso il domicilio del paziente positivo dopo che questo è stato sottoposto a quarantena.









- Verification test:
 - Message Authentication and Integrity Code
 - TIMESTAMP validation
 - Timeout on right message receipt
- Scoring based on TIMESTAMP





